Mobile Communication Network Architecture (MCNA) Architecture Report

(A040)

DOCUMENT NUMBER:	RELEASE/REVISION:	RELEASE/REVISION DATE:
D794-10184-1	**Rev A**	7/25/2005

Export Compliance Notice

This document has been reviewed and approved for release to ALL by Export Compliance.
Log ID: PW-05-193
Review Date: 10/18/05
Additional questions should be addressed to your designated Boeing Export Compliance Administrator.
Richard M. Kling, 206-679-9284

CONTENT OWNER:

GCNSS Systems Engineering Team
Phantom Works ANCO (9S-7S-73CN)

All future revisions to this document must be approved by the content owner before release.

Document Information

Document Type	Original Release Date	Contract Number (if required)
Informal	3/10/2005	XX
Preparing Organization (if different from owning organization)		**Hardware and Software Used**
XX		IBM PC Microsoft Word
Location of Software Files (optional)		
Boeing Web URL (optional)		
Notes and Limitations (optional)		

Signatures for original release

AUTHOR:	Al Sipe		
	Sign and type: First Name MI Last Name	Org. Number	Date
APPROVAL:	John W. Moore		
	Sign and type: First Name MI Last Name	Org. Number	Date
DOCUMENT RELEASE:			
	Sign and type: First Name MI Last Name	Org. Number	Date

Table of Contents

List of Figures

List of Tables

1 INTRODUCTION

1.1 MCNA Overview

The Mobile Communication Network Architecture (MCNA) encompasses the aggregate of all air-ground (A-G) and air-air (A-A) voice, video and data communication capabilities in support of communications, navigation and surveillance (CNS) services for Air Traffic Management (ATM) operations. MCNA is specifically concerned with the support of Air Traffic Safety (ATS) and Airline Operational Communications (AOC) services, but nature of MCNA should provide for common infrastructure to also support Airline Administrative Communications (AAC) and Airline Passenger Communication (APC) services. Like System Wide Information Management (SWIM), MCNA is a key enabling technology for transformation of the National Airspace System (NAS) towards Network Centric Operations (NCO). The MCNA effort represents a System of Systems Engineering (SoSE) based evaluation of MCNA. The specific focus of this effort is the development of the requirements, architecture and associated transition plan necessary to assure that the air-ground and air-air communications capabilities will support of the needs of SWIM-enabled applications (SEA) to provide NCO. The goal of this effort is to develop an integrated SoSE approach and technology development roadmap that will provide guidance for ongoing and planned NASA Glenn Research Center (GRC) and FAA research activities including NASA GRC's Advanced CNS Architectures and System Technologies (ACAST) Project and NASA Airspace Systems Program's proposed initiative for the Transformation of the NAS (TNAS).

The MCNA nomenclature was introduced within the Statement of Work (SOW) of this GCNSS II contract task. As such, it is a common misconception that MCNA refers solely to the "vision" of mobile communications capabilities intended to support the most demanding SWIM-enabled applications including cockpit integration. In fact, all communications to mobile networks in the NAS, such as1090 Extended Squitter (ES), Aeronautical Communications Addressing and Reporting System (ACARS) and Future Air Navigation System (FANS) are all existing components of the MCNA. In time, these components will likely be augmented by Aeronautical Telecommunications Network (ATN) over Very High Frequency (VHF) Digital Link Mode 2 (VDLm2) and VDLm3, Universal Access Transceiver (UAT) and broadband satellite communications (SatCom). Eventually, the NAS will be supported by the suite of enhanced datalink services recommended by the Future Communication System (FCS). The key aspect of MCNA is that it extends voice and data communications to the aircraft during all phases of flight. Figure 1 illustrates how MCNA fits in the Common Data Transport (CDT) portion of the SWIM and thereby supports NCO.

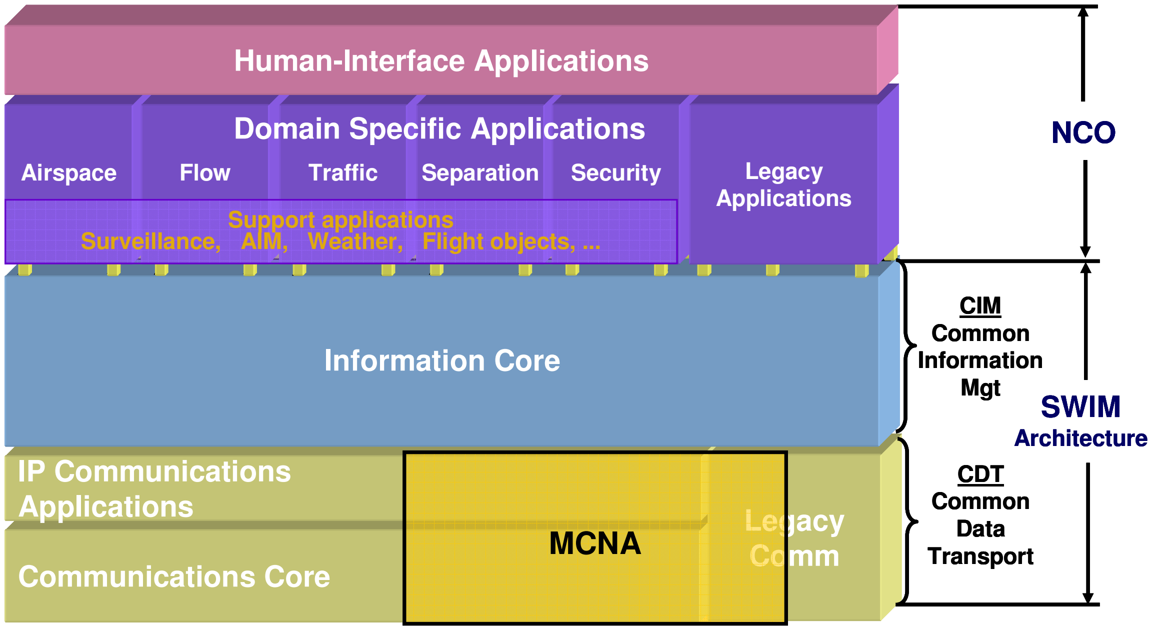

Figure 1: Relationship of MCNA to SWIM and NCO.

While the goal of MCNA is to extend the reach of SWIM information nodes to all mobile elements of the NAS, this does not mean, even in the MCNA long-term vision state, that all communications to and from the aircraft will use SWIM as the means of information exchange. Basically, SWIM will enable the ubiquitous sharing of information between applications. The sharing of information is a result of integrating applications via common mechanisms. SWIM will support multiple integration frameworks (i.e., .NET, J2EE, CORBA, Web Services) and platforms (i.e., Windows, Linux, etc.) for flexibility and evolutionary reasons. The SWIM environment will enable both anticipated and non-anticipated users of information, with anticipated users defined primarily at build-time and unanticipated users defined primarily at run-time. But the fact that the SWIM environment will support and even promote ubiquitous information sharing doesn't mean that all applications should exchange all information with all other applications. Only authenticated and authorized users of information will be allowed to access it, as determined by the "owner" of the information source.

In early SWIM development and deployment spirals, a wide variety of existing information exchange mechanisms and associated communications links will continue to coexist alongside the new SWIM mechanisms. This will be done for both reliability/availability and backwards compatibility reasons. In some cases, it may make sense to retain information exchange mechanisms outside of SWIM beyond the initial spirals. The desirability of these out-of-band information exchange mechanisms will, in general, be greater for application groups that are tightly coupled, synchronous, unlikely to change and unlikely to be expanded. But this decision will be decided on a case-by-case basis and will require a thorough analysis. In most instances the information exchange mechanisms offered by SWIM will be sufficient.

1.2 Purpose and Scope

The sub task of the MCNA effort documented in this report is the development of an architecture that integrates current and future A-G and A-A communication links into a system-of-systems communication network. Special attention is given to the disparate networking protocols and link technologies that must by integrated by this architecture to provide communication services that can meet more stringent performance requirements than any individual A-G or A-A communication link.

The MCNA physical architecture is composed of the following elements which are notionally depicted in Table 1 and Figure 2. As can be seen from the notional physical architecture, the MCNA is specifically concerned with addressing issues related to the integration of multiple disparate radio links and networking protocols. Furthermore, the MCNA architecture is concerned with seamless integration into the SWIM concept.

Table 1 MCNA Architecture Elements

Airborne Architecture Elements	Terrestrial Architecture Elements
Airborne host	Terrestrial host
Airborne router	Terrestrial router
Airborne message router	Terrestrial message router
Airborne gateway	Terrestrial gateway
Airborne modem/radio	Terrestrial ground station
Airborne firewall	Network Operations Control Center (NOCC)
	Domain Name Server (DNS)

This task focuses on three key elements of the MCNA architecture: candidate A-G and A-A links, network architecture and the avionics architectures that comprise the aircraft portion of the other two components. Initially, the candidate links are summarized and compared. With this perspective, a proposed MCNA network architecture is defined. Specific consideration is provided for those elements of the MCNA network architecture required to extend SWIM to/from the aircraft to support NCO. The dependencies between the avionics architecture and the MCNA network architecture are described. The avionics architecture includes discussion of the avionics transition as this is one of the most critical aspects to address when considering avionics issues. Finally, the architecture is mapped to the requirements and discussion is provided regarding the ability of the MCNA architecture to address NAS shortcomings defined during the previous phase of the GCNSS contract.

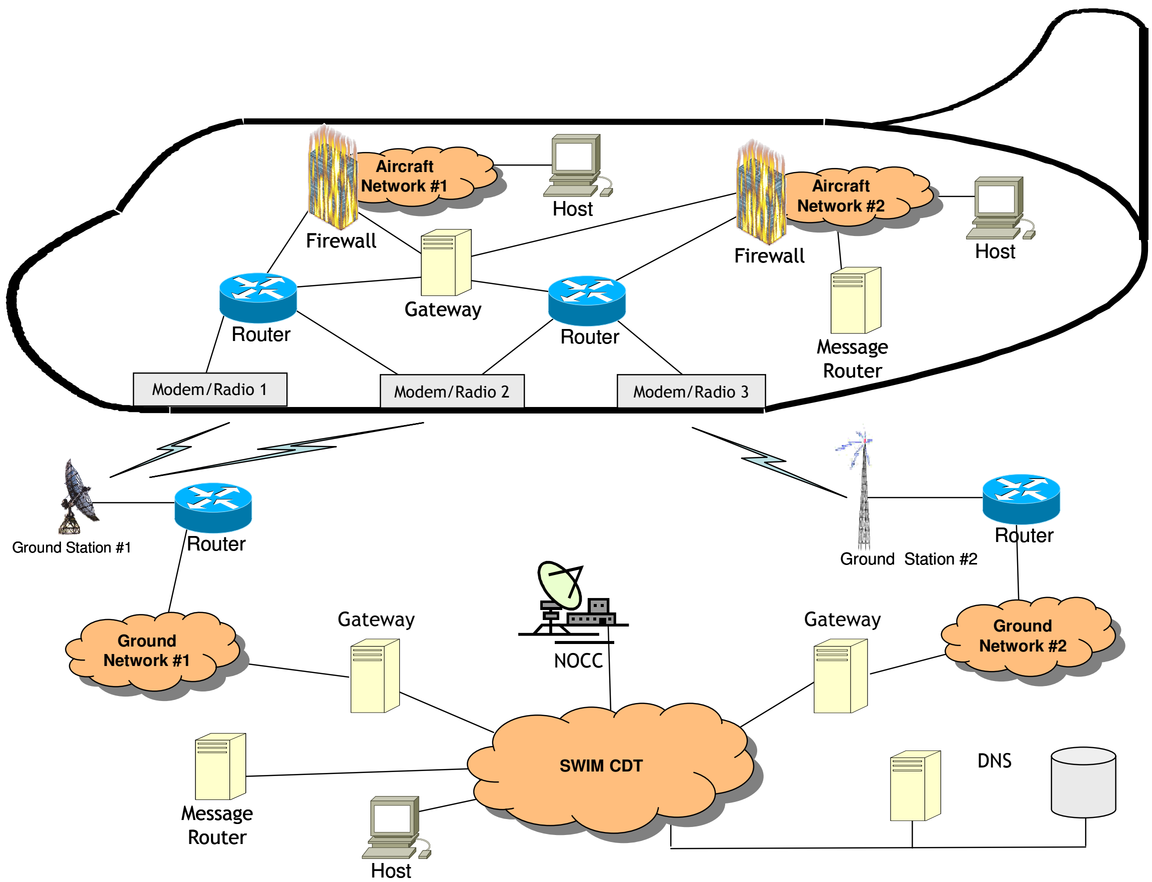

Figure 2 Notional Physical Architecture for MCNA

1.3 Systems Engineering (SE) Process

One view of the applicability of architecture definition activities in the development process is shown in Figure 3. Here, the system development process, as defined in the FAA Systems Engineering Manual (SEM), is used as a reference. The arrow in the figure points out where architecture definition supports the development process. Architecture definition is one of the preliminary steps in the SE task defined as synthesis within the FAA SEM.

The MCNA effort was not intended to produce a comprehensive set of systems engineering products so much as to conduct a high level, broad scope survey of the MCNA concept with the intention of identifying key targets of opportunity for targeted research. As such, this architecture report does not claim to represent a complete MCNA architecture but rather facets of such and architecture and key considerations when pursuing a more detailed architectural MCNA study. The candidate link evaluation effort reviewed the results from the FCS technology prescreening and adapted those results to include existing candidate links and additional evaluation criteria from a SoSE perspective such as networking protocols and interoperability considerations at multiple levels. Furthermore, this effort provided mechanisms to evaluate individual candidate links with the mindset that a total solution would likely consist of the aggregation of multiple candidate links rather than selecting a single candidate link the best meets the overall aggregation of needs.

The network architecture study provides a survey of select topics relevant to a mobile networking architecture, including: routing, mobility, multihoming, policy based routing, multicast, QoS, security and network management. In additional, special emphasis was placed upon defining the relationship between MCNA and SWIM and addressing the inherent need for interoperability that MCNA must address. Network layer interoperability between ACARS, CLNP and IP is considered at the link layer, the network layer and at the application layer through a message transport service provided by SWIM.

The avionics architecture effort summarizes current architecture characteristics and proposes a vision state avionics architecture that extends recent ARINC 664 efforts to address the MCNA considerations introduced from this effort. Additional consideration is provided for avionics transition concepts and certification issues.

Due to the nature of this study, schedule and resource constraints required the implementation of a parallel systems engineering approach. As a result, the integration between SE products is less than optimum. It is anticipated that a subsequent iteration of the SE process would greatly remedy this critical shortcoming.

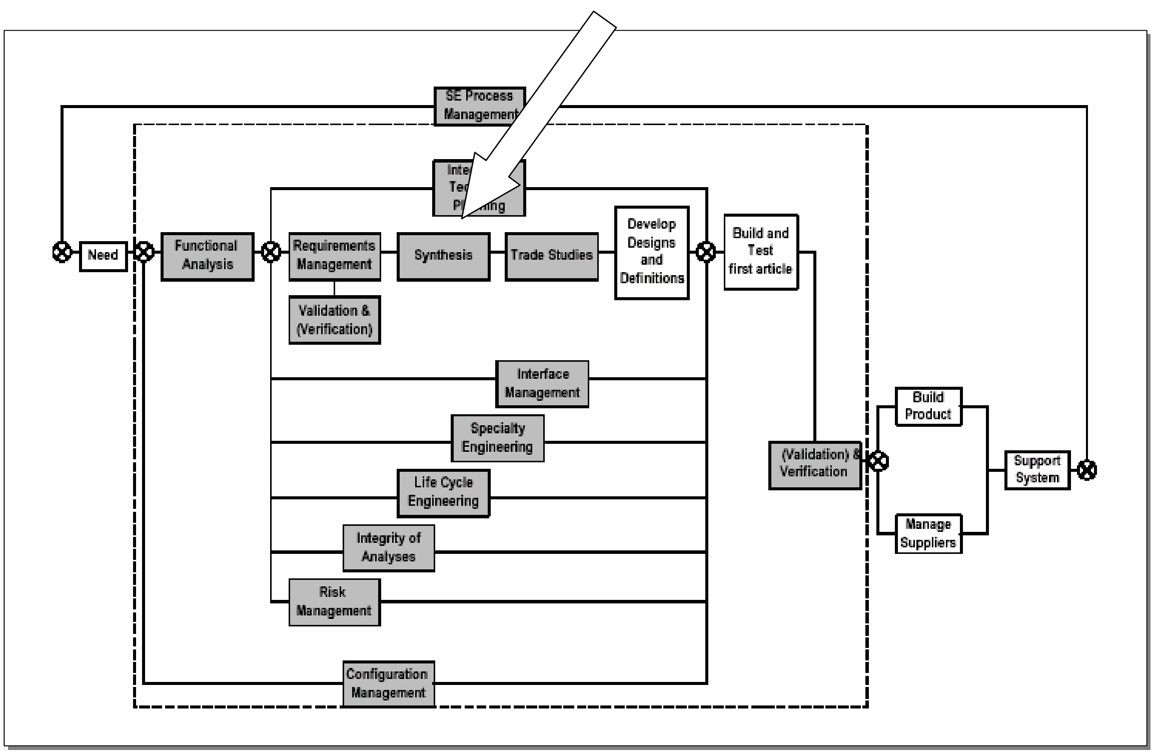

Figure 3 Architecture Definition within the FAA SE Process

1.4 Document Roadmap

This section provides an overview of the MCNA effort and introduces the Architecture report and its relationship within the overall MCNA effort.

Section 2 describes the candidate air-ground and air-air links evaluated as part of the MCNA architecture effort.

Section 3 outlines the MCNA network architecture providing descriptions of how each of the main MCNA functions will be addressed.

Section 4 described current and proposed avionics architectures as necessary to support the MCNA concept.

Section 5 provides a mapping between the defined MCNA architecture and the requirements.

Section 6 describes how the proposed MCNA architecture addresses the shortcomings defined during GCNSS I.

Section 7 summarizes the conclusions and recommendations from this MCNA requirements report.

Section 8 describes the references used for the development of this report.

Section 9 provides a list of Acronyms used in this report.

2 MCNA COMMUNICATION LINK CANDIDATES

2.1 Scope

The candidate links represent an aggregate of disparate wireless communications systems that can be used to inter-connect aircraft and other moving vehicles with ground operations, automations systems or other aircraft. A physical architecture diagram representing the candidate links under consideration for MCNA is shown in **Error! Reference source not found.**. An additional key aspect of the physical architecture is the fact that multiple disparate networking protocols are currently in use. The number of those protocols may increase before eventually converging toward a smaller set of standard network protocols.

ACARS is the predominant networking protocol for aviation air-ground telecommunications. The ATN and its associated protocols were introduced in the 1990's as an international standard. Recently, the ATN protocols were utilized in the US during the brief Miami trials. ATN trails are ongoing in Europe and a key part of the Operational Evolution Plan (OEP) [25] and the National Air Space (NAS) 5.0 [10] plans of the FAA. However, due to its popularity and commercial success of the internet, the Internet Protocol (IP) is expected to become an important and potentially dominant networking protocol for future Air Traffic Management (ATM) communications. A key aspect of the MCNA architecture is the consideration of these three disparate networking protocols and how they will be accommodate through the lengthy transition process. This consideration is addressed in part within the candidate links discussion as the underlying network protocol as an evaluation factor for each of the candidate links and is addressed in much greater detail as part of the network architecture discussions in Section 3.

2.2 Candidate Links Table

A table has been compiled that identifies and characterizes the various candidate links that are currently available, planned for future deployment and/or proposed future links. Candidate links are classified into:

- Air-Ground Communications: Terrestrial wireless communications
- Satellite Communications: Wireless communications via satellite systems
- Air-Air Communications: Wireless communications systems that include direct communications between aircraft. Many of the systems that provide air-air communications also provide air-ground communications but most are categorized under the air-air communications grouping.

- Airport Communications: Shorter range wireless communication systems that often take advantage of the limited physical propagation distance to provide wider bandwidth datalink communication services.

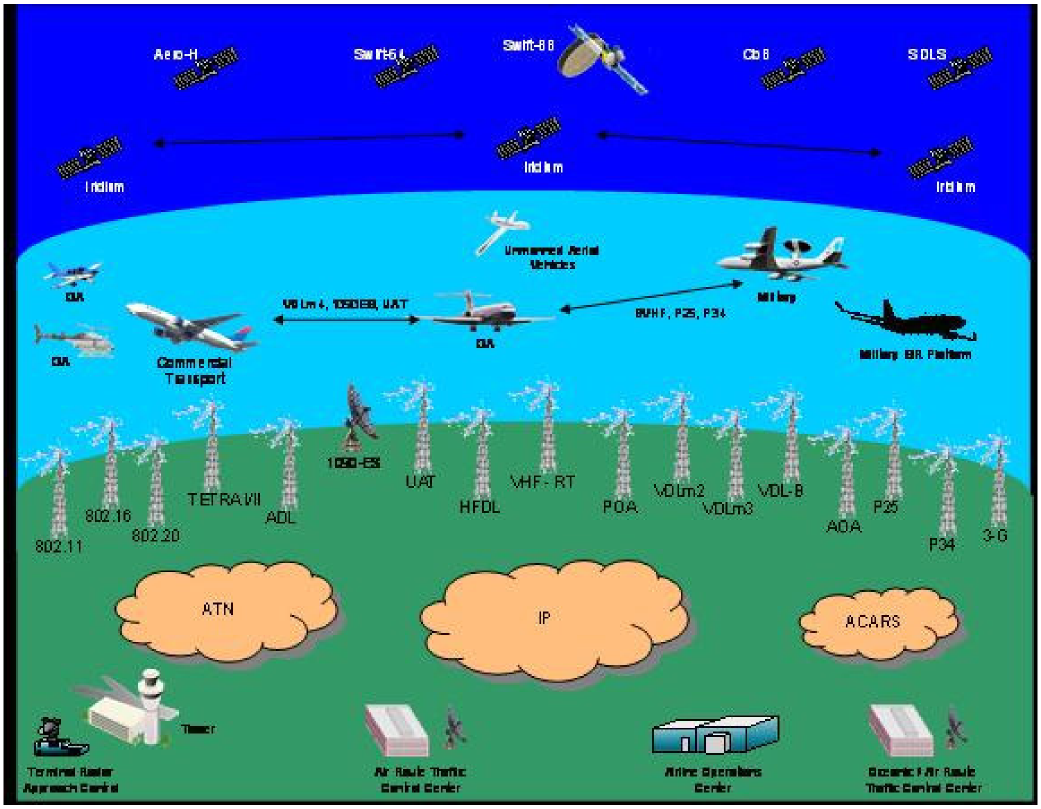

Figure 4 MCNA System of Systems View

Table 2 aggregates information about each of the candidate communications links, organized into the categories described above. Most of the candidates were extracted from the initial findings and recommendations to the FAA under the technology pre-screening assessment of the Future Communications Study (FCS), conducted for NASA Glenn Research Center by ITT Industries. However, additional links were also included, mostly to account for existing systems that were not described in the aforementioned study. For each of the identified candidate links, the following characteristics were identified:

- **Link ID Number** – This is a unique integer reference for each candidate link for use within the candidate link database and as a general reference.

- **Associated networking protocols** – This key characteristic has resulted in defining sub-classes for candidate links based upon which networking protocol is supported by the Air-Ground (A-G) link. Given the desire within the FAA's SWIM Program to eventually migrate towards IP, the supported networking protocols are key characteristics.

- **Spectrum** – The current or anticipated spectrum band(s) for operation of the candidate link. Availability and Aeronautical Mobile (Route) Service (AM(R)S) or Aeronautical Mobile Satellite (Route) Service (AMS(R)S) designation of the selected spectrum is a key factor.

- **System Wide Information Management (SWIM) Support** – This qualitative characteristic is intended to describe the degree to which the candidate link is anticipated to enable SWIM-based services, and Network-Centric Operations (NCO).

- **Availability (date)** – Rough estimate of the year by which the proposed candidate link might be available.

- **Communication Services** – Each column represents a communication service class. If a candidate link can support some or all of the service levels within that class a number is entered into the column representing the most stringent service level that the link supports within that service class. Lower numbers represent more stringent service requirements. Therefore, a system that can meet the requirements of service Level n within a class can by definition support service level n+1, n+2, etc. Consequently, an entry of one (1) within a cell suggests that the system can support all service levels within a service class.

- **Airspace Domain** – Each of the airspace domains are represented by individual columns. These cells contain a Boolean variable (Y/N) that represents whether a particular candidate link provides service with each airspace domain.

- **Aircraft Class** – Boolean characterization representing the support of various aircraft types by each of the candidate links. This evaluation is much more subjective than most of the other characterizations and requires much more detailed understanding of the SWIM and MCNA Concepts of Operations in order to properly evaluate.

- **Cost** – Divided into four sub-categories: System, Operation and Maintenance (O&M), Service and Avionics. All candidate links should have an avionics cost but the use of commercial systems impose service costs while privately owned systems incur system and O&M costs. Cost rankings for these candidate links were based upon the expertise and internal review of the MCNA team.

- **System Cost** – The cost to design, develop and deploy the candidate link.[1]

- **O&M Cost** – Operations and Maintenance cost includes, technology refresh, consumables (power, land or building lease, etc) and manpower.

- **Service Cost** – For commercial systems, a service provider such as ARINC or SITA incurs the costs of the system and O&M. In turn, the service provides charges airlines a service fee (typically based upon usage). The actual fee structure for any system is very complex and based upon service packaging, volume and negotiation. For simplicity, rough comparative values are employed.

- **Avionics Cost** – Each candidate link requires the installation of avionics and an antenna on the aircraft. Cost is most dependent upon volume, antenna and certification level. This introduces complexity since a given candidate link might have different antenna and certification level requirements to support various communication services, levels and aircraft types.

- **Risk** – Three of the following risks are derived from the FCS evaluation criteria. An additional risk, political, was introduced to more fully characterize the risk environment.

  - **Technology Readiness Level (TRL)** – NASA scale for technical maturity of a concept or system (1 to 9 with 9 being the most mature). Mapped for this work to a subjective scale of (high (H), medium (M) and low (L))

  - **Standardization** – Availability of published standards for the candidate link.

  - **Certification** – Anticipated complexity and effort to achieve link and avionics certification (approval).

  - **Political** – Subjective assessment of the magnitude of political differences of opinion regarding the suitability of the candidate link for aeronautical applications.

[1] The system cost, particularly for terrestrial air-ground systems is tightly coupled with the required service availability due to its influence on the required density of ground stations. Since different communication service classes and levels have different availability requirements, an additional degree of freedom is introduced into the cost model. This additional degree of freedom is only noted due to the added work and complexity to model this for all of the candidate systems.

- **Link Type –** Three link types are identified, Air-Ground (A-G), Air-Air (A-A) and Air-Space (A-S). Typically, A-G and A-S are mutually exclusive, but some A-G systems also support A-A services.

Table 2 Candidate Links Table

General Characteristics						Communication Services												Airspace Domain							Aircraft Class						Risk				Cost 1 - 5				Link Type		
Candidate Link Type	Link ID Number	Associated Networking Protocols	Spectrum	SWIM Support (3 is highest)	Availability (date)	Party-line Voice	SA Voice	Broadcast Voice	Data Messaging	Trajectory exchange	Broadcast to Aircraft	Broadcast From Aircraft	Ground to Air Data	Air to Ground Data	Air to Air Data	Video Exchange	Vehicle Command and Control	Gate	Surface	Terminal	En-route	Remote	Oceanic	Polar	Transport	Cargo	Military	UAV/ROA	GA - Business	GA - Personal	TRL	Standardization	Certifiability	Political	System	Maintenance	Service	Avionics	A-G	A-A	A-S
Air-Ground Communications																																									
VHF Analog Voice	1	NA	VHF	0	2005	1		1										Y	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y	L	L	L	L	0	4	0	1	Y	Y	N
HF Analog Voice	2	NA	HF	0	2005		3											N	N	N	N	Y	Y	Y	Y	Y	Y	N	N	N	L	L	L	L	0	2	0	3.5	Y	Y	N
Plain old ACARS (POA)	3	ACARS	VHF	1	2005				3									Y	Y	Y	Y	N	N	N	Y	Y	N	N	Y	N	L	L	L	L	0	0	3	2	Y	N	N
VDLm2	4	ACARS	VHF	1	2005				3				3	3				Y	Y	Y	Y	N	N	N	Y	Y	N	N	Y	N	L	L	L	L	0	0	2.5	2.5	Y	N	N
	5	CLNP	VHF	2	2010			2	2	2			3	3				Y	Y	Y	Y	N	N	N	Y	Y	N	N	Y	N	L	L	L	M	0	0	2.5	2.5	Y	N	N
	6	IP	VHF	2	2010			2	3		3	3	3	3				Y	Y	Y	Y	N	N	N	Y	Y	N	N	Y	N	M	H	H	M	0	0	2.5	2.5	Y	N	N
	7	NA (VDL-B)	VHF	2	2005						2							Y	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y	L	L	L	L	2	2	0	2	Y	N	N
VDLm3	8	CLNP	VHF, DME	2	2020				1	1							2	Y	Y	Y	Y	N	N	N	Y	Y	N	Y	Y	N	L	L	L	H	4	3	0	2.5	Y	N	N
	9	Voice		1	2015	1		1										Y	Y	Y	Y	N	N	N	Y	Y	N	Y	Y	N	L	L	L	H					Y	Y	N
HFDL	10	ACARS	HF	1	2005				3									N	N	N	N	Y	Y	Y	Y	Y	Y	N	N	N	L	L	L	L	0	0	3.5	3.5	Y	N	N
	11	CLNP			2010																																				
3G	12	IP	DME	3	2020	3	2	1	1	1	1	1	1	1		2	2	Y	Y	Y	Y	N	N	N	Y	Y	N	N	Y	Y	M	H	H	M	3	3	0	3	Y	N	N
Satellite Communications																																									
Aero-H	13	ACARS (data-2)	AMSRS	1	2005		2		2	2								Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	L	L	L	L	0	0	5	4.5	N	N	Y
	14	CLNP (data-3)			2010																										M	M	M	L							
	15	IP (data-3)			2010																										M	M	M	M							
Swift-64	16	IP	AMSRS	1	2005		3	1	3		3	3	3	3			3	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	L	H	H	M	0	0	3	4	N	N	Y
Swift-Broadband	17	IP	AMSRS	3	2010	3	2	1	1	1	2	3	1	1		2	2	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	M	M	M	M	0	0	2	4	N	N	Y
SDARS	18	IP	S-Band	2	2015			1			2							Y	Y	Y	Y	Y	N	N	Y	Y	N	N	Y	Y	M	H	H	M	0	2	0	1.5	N	N	Y
SDLS	19	NA	AMSRS	2	2015	3	1	1	1	1	2	3	1	1				Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	H	H	H	H	2	3	0	3	N	N	Y
Iridium	20	Layer-2	L-Band	1	2005		3		3		3							Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	L	M	H	H	0	0	2.5	2	N	N	Y
Connexion by Boeing	21	IP	FSS	3	2005	4	3	2	3		3	3	3	3		2	3	N	N	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	L	H	H	H	0	0	2	6	N	N	Y
Air-Air Communications																																									
1090-ES	22	CLNP	DME	1	2010				2	2					1			N	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y	N	L	L	L	L	1	1	0	2	Y	Y	N
	23	Layer-2	DME	1	2005						1	1						Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	L	L	L	L					Y	Y	N
UAT	24	Layer-2	DME	2	2010						1	1						N	Y	Y	Y	Y	N	N	N	N	N	N	Y	Y	L	L	M	M	3	3	0	3	Y	Y	N
VDLm4	25	CLNP	VHF	1	2010							1			1			N	N	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	L	L	M	H	0	0	0	3	N	Y	N
B-VHF	26	CLNP	VHF, DME	3	2025	1	1	1	1	1			1	1	1		2	Y	Y	Y	Y	N	N	N	Y	Y	N	Y	Y	N	H	H	H	M	4.5	3	0	3	Y	Y	N
	27	IP				1	1	1	1	1	1		1	1	1		2																								
P-25	28	IP	DME	1	2020	1	1	1	3									Y	Y	Y	N	N	N	N	Y	Y	Y	N	Y	Y	M	H	H	M	4	3	0	3	Y	Y	N
P-34	29	IP	DME, MLS	3	2025	2	2	1	1	1	1	1	1	1	2	2	2	Y	Y	Y	Y	N	N	N	Y	Y	N	Y	Y	N	M	H	H	M	5	4	0	3	Y	Y	N
Airport Communications																																									
Airport Data Link (ADL)	30	NA	MLS	3	2025	2	1	1	1	1	1	3	1	1		1	1	Y	Y	N	N	N	N	N	Y	Y	N	N	Y	Y	H	H	H	M	2	2	0	3	Y	N	N
IEEE 802.11	31	IP	ISM	3	2010			2	3		3		3	3				Y	N	N	N	N	N	N	Y	Y	N	N	Y	Y	L	M	H	M	1.5	1.5	0	2	Y	N	N
	32	CLNP			2015			2	3				3	3																											
IEEE 802.16	33	IP	ISM, MLS	3	2020	2	1	1	1	1	1	1	1	1	1	1	1	Y	Y	N	N	N	N	N	Y	Y	N	N	Y	Y	L	H	H	M	2	2	0	3	Y	N	N
	34	CLNP				2	1	1	1	1			1	1	1	1	1																								
IEEE 802.20	35	IP	ISM, DME	3	2025	2	2	1	1	1	2	2	1	1		2	2	Y	Y	N	N	N	N	N	Y	Y	N	N	Y	Y	M	H	H	M	2	2	0	3	Y	N	N
	36	CLNP				2	1	1	1	1		2	1	1		2	2																								
TETRA I/II	37	IP	DME	2	2025	1	1	1	1	1	1	1					1	Y	Y	N	N	N	N	N	Y	Y	N	N	Y	Y	M	H	H	M	2	2	0	3	Y	N	N

2.3 Air-Ground Communication Systems

The following sub-sections offer brief descriptions of some of the key characteristics worthy of mention for each of the identified candidate links.

2.3.1 VHF Systems

Very High Frequency (VHF) systems represent the majority of current or planned air-ground communication systems. The crowding of the VHF band has resulted in the investigation of alternate spectral bands in which to deploy new communication systems.

2.3.1.1 VHF Analog Voice

VHF Analog voice is currently the dominant means of Air Traffic Management / Communication Navigation & Surveillance (ATM/CNS) communications. Based upon radio technology from early last century, these half duplex channels result in a shared "party-line" voice communication media that has been adapted through procedures to become a useful tool for pilots and controllers. While most of the future operational concepts look to move toward the use of data as the primary means of communication with voice communications by exception only, VHF analog voice will remain for many decades as a backup communication system and for primary support of legacy aircraft (especially GA) that will not realize sufficient benefits to upgrade equipage.

VHF analog voice provides party-line voice services, broadcast voice services and can also provide pilot-pilot voice service. As such, it could therefore be classified as an air-air system. However, since this service is not really used operationally other than as an emergency back up capability, it was grouped with the air-ground communication systems.

2.3.1.2 Plain Old ACARS (POA)

POA is the dominant data messaging system used today for aviation applications. The link provides only 2.4kbps channel burst rate with a Carrier-Sense Multiple Access (CSMA) Media Access Control (MAC) protocol that does not offer any Quality of Service (QoS) mechanisms at layer-2 and therefore limits the applicability of this system to AOC, AAC and occasionally APC messaging services. However, given the fact that this has been the only available datalink system for many years, certain Air Traffic Service (ATS) have in fact been implemented over POA such as Flight Information Services (FIS) and Departure Clearance (DCL) services.

POA was designed to support the ACARS protocols and given the limited bandwidth of this candidate link, coupled with the emergence of a more bandwidth efficient alternative (VDLm2), it does not make sense to consider modification to support Connection Less Network layer Protocol (CLNP) or IP.

2.3.1.3 VDLm2 (AVLC)

VHF Data Link Mode 2 (VDLm2) is a more bandwidth efficient VHF datalink that has recently grown in popularity. VDLm2 provides 31.5kbps channel burst rate within the same 25kHz channels used for POA. The link layer protocol associated with VDLm2 is Aviation VHF Link Control (AVLC) which is a modification of the popular High-Level Data Link Control (HDLC) protocol.

Similar to POA, AVLC uses CSMA MAC and consequently does not provide any layer-2 QoS mechanisms that allow prioritization of packet delivery from the individual aircraft to the ground. This is a somewhat contentious issue because it suggests that AVLC does not meet ICAO requirements for an ATS datalink. However, both Europe and the US have significant plans to deploy ATS datalink services over AVLC with operational procedures to meet safety assurance requirements. It is anticipated that the scope of datalink operations may be restricted due to this limitation of AVLC.

CLNP over AVLC - AVLC was originally developed as part of the ATN in support of CLNP packet transport. This protocol combination was selected for the Miami Controller Pilot Datalink Communication (CPDLC) trials and for the Eurocontrol Link2000+ CPDLC trials. The packet prioritization from CLNP provides reasonable QoS mechanisms on the forward link (from ground stations to the aircraft) but can only differentiate the order of delivery between packets from a single aircraft on the return link (from the aircraft down to the ground).

ACARS over AVLC (AOA) – After the introduction of VDLm2 and AVLC, the bandwidth efficient nature of this candidate link (especially relative to POA) captured the attention of the ACARS community and a Sub-Network Dependent Convergence Function (SNDCF) was established to transport ACARS messages over AVLC. Given the reduced regulatory and certification restrictions, AOA has become more popular and widely adopted. Both Datalink Service Providers (DSP) have either completed or are in the process of upgrading their datalink networks to support AOA services.

IP over AVLC – Recently, SITA has been conducting research and developing demonstrations to support the transport of IP packets over the VDLm2 AVLC link. This effort is still a very preliminary but indicative of future directions. However, it is important to note that regulatory restrictions on spectrum usage will limit the supported applications on this link. Since this VHF band is allocated as AM(R)S, it can only be used to support ATS and AOC applications

2.3.1.4 VDLm3

VHF Data Link Mode 3 (VDLm3) is an alternate VHF datalink protocol developed for the FAA to provide simultaneous support of voice and datalink service. In contrast with the European solution of 8.33kHz channelization for VHF voice, VDLm3 relies upon voice digitization and Time Division Multiplexing (TDM) to achieve similar spectral efficiency increases. Furthermore, this technology provides the ability to flexibly divide an existing voice channel into multiple combinations of voice and data sub-channels.

VDLm3 also introduces more functionality within the MAC to provide Layer-2 QoS mechanisms that overcome the shortcomings identified with VDLm2 (regarding the CSMA MAC). The largest shortcoming of VDLm3 is uncertainty of its deployment given the increasing deployment of 8.33kHz channelization. While a superior technology for integrating voice and data services, 8.33kHz analog voice achieved a more successful deployment (in Europe). Accordingly, many airlines have already upgraded their equipage to support 8.33kHz and consequently have little incentive to adopt an alternate technology that would result in additional equipage costs.

At this point, the general sentiment (supported by NASA's FCS technology pre-screening recommendations to the FAA) is that new technologies should not be introduced into the VHF band. If this guidance is followed, VDLm3 may provide a wealth of datalink technology elements (such as an approved vocoder[2]) but would be unlikely to exist as a stand-alone system, at least in the VHF band.

2.3.1.5 VDL-B

VDL-Broadcast (VDL-B) is a variant of the VDLm2 physical layer (PHY) used for the broadcast of information such as FIS. VDL-B does not support the transport of any network packets but instead broadcasts information as a layer-2 service.

2.3.2 HF Voice

The HF Voice service relies upon the propagation phenomena experienced by HF waves in the ionosphere to achieved extended range communications in Oceanic and Polar airspace domains. While the HF communication service is voice, the pilots do not communicate directly with controllers. Instead, a service provider talks directly with the pilots and relays messages from/to controllers via datalink. As such, the HF voice service does not qualify as Direct Controller to Pilot Communications (DCPC). The HF channel is typically very noisy. As such, pilots prefer not to monitor the HF channel. Instead, a Selective Calling (SELCAL) function has been implemented that wakes up an HF radio when a message needs to be sent to a particular aircraft.

---

[2] The NexCom program selected and certified a DVSI vocoder for use over narrowband datalinks. This certification effort could be leveraged for future programs to save cost and schedule.

2.3.3 HFDL

HFDL provides low availability data link services within Oceanic and Polar airspace domains. The data rate is limited to 1.2kbps and both reliable link service (RLS) and data link service (DLS) specifications have been developed. ACARS over DLS currently exists for AOC services. In order to transport CLNP packets over HFDL, the RLS service must be employed. This service is not yet available and no near term plans to provide such a service have been publicized. Likewise, no plans exist to support IP services and given the limited bandwidth of this candidate link it would not be recommended to pursue such accommodations.

2.3.4 3rd Generation Cellular (3G)

Third generation cellular systems are slowly being deployed commercially for non-aviation telecommunication services and show much promise in combining voice and data services. Given the significant commercial backing in the development of detailed specifications, consideration has been given towards leveraging these standardization efforts to define next generation aviation communication systems. Several shortcoming of this route include:

- These specifications were not developed for safety of life applications and would need to be approved accordingly. The complexity of these specifications would result in a significant analysis effort to achieve such certification / approval.
- 3-G was not developed to support the range and mobility speeds necessary to support aircraft.

While 3-G systems tout data rates of multiple Mbps, these link conditions can only be achieved over relatively short ranges. Given the ranges required for En-route communications (200+ nmi) the maximum data rate that can be achieved is strongly influenced by the antennas employed. With omni-directional antenna on both the ground and aircraft, only tens of kbps can be achieved at this range at VHF. The peak data rate can be increased somewhat with more complex base station antenna, but the only way to achieve high bandwidth channel throughput is to employ directive antennas on the aircraft. However, such antennas would introduce high avionics and installation cost and downtime issues.

2.3.5 Future Terrestrial System

The Future Terrestrial System is a placeholder for a system to be developed in the distant future to either address the aggregate of all communication needs or at least address those requirements not otherwise accommodate by the candidate links.

2.4 Satellite Communications Systems

The characteristics of the satellite communication systems considered are also detailed in Table 2. Over the last decade, SatCom has become a critical part of Oceanic communications in the aviation industry. Lately, new SatCom offerings and concepts have evolved that plan to address both passenger communications needs and ATS/AOC. The following sections highlight key characteristics of the evaluated systems.

2.4.1 Inmarsat Aero-H

The Inmarsat Aero-H service is the communications foundation for the Future Air Navigation System (FANS) service offerings that have become pervasive in Oceanic airspace. FANS consists of CPDLC and Automatic Dependent Surveillance – Addressed (ADS-A). Aero-H provides Layer-2 packet prioritization over narrowband links (10.5kbps or less). The Demand Assigned Multiple Access (DAMA) scheme employed for the Aero-H packet data service effectively meets the ICAO requirements but also introduces significant latency. This latency has been acceptable for the classes of services and operations conducted to date. However, the latency is becoming a limiting factor in supporting future datalink operational concepts.

Aero-H also provides selective addressed (SA) voice services. Currently this service is only used as an emergency backup if no other means are available for voice communication. However, recent efforts have begun to allow Aero-H voice as a primary means of communication in Oceanic airspace.

Inmarsat Aero-H requires a relatively large phased array antenna, expensive avionics and has classically been a relatively expensive service. These factors have impeded the adoption of this candidate link outside of trans-oceanic aircraft.

2.4.2 Inmarsat Swift-64

Swift-64 is a recent service offering from Inmarsat over the existing constellation of Inmarsat-3 satellite that provides both ISDN-compatible circuit switched datalink services at 64kbps and packet switched services at comparable data rates. Swift-64 was developed primarily for passenger services rather than safety of life services. However, the performance of the link sparked a wide array of interest in providing safety of life services over this link. Given the pending deployment of Inmarsat Swift-Broadband, most safety of life services over Swift-64 concepts have been deferred until the launch of the Swift-Broadband service.

2.4.3 Inmarsat Swift-Broadband

Swift-Broadband is the next generation of Swift-64, based upon a new constellation of much more capable Inmarsat (I-4) satellites. This service provides ~500kbps symmetric channel throughput to an antenna that is equivalent to previous Inmarsat Aero systems. The Swift-Broadband service combines both voice and data onto a common bearer and provides the hooks to implement the Universal Mobile Telecommunications System (UMTS) priority and pre-emption mechanisms at a later date.

Initially, Inmarsat was focusing Swift-Broadband for passenger services but lately they have begun applying more effort towards addressing the support of safety services. Furthermore, an ARINC781 specification development effort is underway to define lower cost SatCom avionics solutions with support of both cockpit and cabin services.

2.4.4 SDLS

SDLS is a proposal by ESA and Eurocontrol to develop a satellite based solution for ATS datalink within the European Union (EU). To date, this effort has been mostly research oriented. It does not appear likely that this effort will result in the deployment of a new satellite constellation merely to support ATS services within the EU. Recently, there has been discussion about SDLS leasing transponder spectrum from existing AMS(R)S providers to create their proposed service offering. In many respects this concept is similar to the overall goals of MCNA to provide a mechanism to form more stringent communication service classes and levels through the aggregation of multiple existing systems and links. However, SDLS is considered the integration of systems at the physical layer which is much more restrictive than integration of systems at either the network layer or application layer as proposed by MCNA. Furthermore, if SDLS is planning to lease spectrum from Inmarsat satellite to support a custom air interface protocol, it seems logical to first investigate if comparable services could be provided using the Inmarsat air-interface protocols over their own satellites.

2.4.5 Iridium

Iridium is a truly global satellite communication system providing worldwide coverage, even within the Polar airspace domain. The Iridium system has also been used as part of the Alaska Capstone trials. However, the current Iridium system has limited constellation life and has not publicly presented a viable business plan for constellation replacement beyond ~2014. The potentially limited constellation life may not be significant for GA aircraft due to the modest costs for GA avionics. However, in the case of transport aircraft, airlines expect that installed avionics should provide service for the remaining life of the aircraft. In most cases, this duration is likely to be much greater than the anticipated remaining operational life of Iridium.

Iridium provides circuit switched voice and data services at channel rates of 2.4kbps. Packet data services are also available via Iridium[3] but such a service would probably offer much lower aggregate channel throughput. As such, Iridium could accommodate certain niche MCNA needs, such as polar, oceanic and remote coverage.

[3] See http://www.blueskynetwork.com for flight following equipment and services via Iridium. The Iridium website http://www.iridium.com describes both a Short Message Service (SMS) with a maximum of 160 alpha-numeric characters per message and a Short Burst Data (SBD) with a maximum of 1960 bytes mobile originated and 1890 bytes mobile terminated per message.

2.4.6 Connexion by Boeing (CbB)

CbB is a recent service offering from the Boeing Company focused on providing broadband communication services primarily for passenger services. Recently, CbB has begun investigating regulatory considerations related with providing AOC and eventually ATS services. Depending upon the outcome of this effort, coupled with their commercial viability over the coming years, CbB may prove a useful component of MCNA. One significant shortcoming of the current CbB design is the cost and mass of the avionics and the drag of the associated satellite antennas. However, if their business case can justify these expenses, the pre-existence of this IP-based SatCom link may support a wide range of MCNA-enabled scenarios.

2.4.7 Future SatCom System

Similar to the Future Terrestrial System, the Future SatCom System is a placeholder for a satellite communication system to be developed in the distant future to either address the aggregate of all communication needs or at least address those requirements not otherwise accommodate by the candidate links. Depending upon the timing of the design and deployment of future Inmarsat replacement constellations (Inmarsat-5 and Inmarsat-6) or other commercial communication satellite constellations, the requirements defined for such systems from a gap analysis could be shared with these commercial service providers as recommendations for future needs.

2.5 Air-Air Communication Systems

The following systems include facilities to support direct air-air communications and therefore are listed separately from the Terrestrial links. Many of these candidate communication links also provide Air-Ground communication services.

2.5.1 1090-ES

This link candidate, 1090MHz –Extended Squitter (1090-ES), has been jointly selected by FAA and Eurocontrol as the standard for Automatic Dependent Surveillance - Broadcast (ADS-B) support of transport aircraft. 1090-ES is an extension of the pervasive Mode-S transponder systems common on most Instrument Flight Rules (IFR) equipped commercial aircraft. Since much of the avionics is required for IFR aircraft, the cost to upgrade or modify this surveillance system to support minimal communications functions is rather modest in comparison with many other MCNA candidate link alternatives.

The available bandwidth for 1090-ES is a single 4Mbps time-division-duplex (TDD) channel shared across the NAS. Given the extensive plans to broadcast ADS-B messages from all aircraft at a relatively high update rate, the remaining bandwidth to support other MCNA communication services may prove rather limited. Furthermore, the access interval within En-route airspace would be twelve (12) seconds. This access interval is reduced to five (5) seconds in terminal airspace but in both cases this may prove a significant limitation with respect to the class of services supported.

1090ES is an ICAO approved ATN datalink and therefore supports predominantly CLNP packets. However, the majority of the 1090ES traffic will be ADS-B messages that are transported as a Layer-2 service.

2.5.2 UAT

Universal Access Transceiver (UAT), developed by MITRE, was selected by the FAA as the preferred means of transporting ADS-B messages for GA aircraft. UAT provides random access slots for aircraft to transmit ADS-B messages but also provides TDMA slots for broadcast services such as TIS-B and FIS-B. UAT does not support any network protocols and is therefore severely limited in the range of communication services classes supported.

2.5.3 VDLm4

VDLm4 is another VDL variant popular in certain regions of Europe, mostly as a means to support ADS-B services. VDLm4 is a topic of debate within the international aviation community and therefore is likely to meet severe political resistance in some regions of the world. However, while the world has adopted 1090-ES as the ADS-B candidate link for transport aircraft, the FAA and Eurocontrol have split between UAT and VDLm4 as the preferred candidate link for ADS-B among GA aircraft.

VDLm4 can also support air-ground communications. For the purposes of this study, only the air-air communications services are under consideration. This assumption was made because it reduces the infrastructure cost for VDLm4 deployment and it was not clear that VDLm4 was under serious consideration for any additional applications support.

2.5.4 B-VHF

Broadband VHF (B-VHF) is a new research effort within Europe to evaluate new air-ground communication system concepts for ATS and AOC applications. The predominant focus of this effort is on a modulation/multiple access scheme, multi-carrier code division multiple access (MC-CDMA), that would allow the deployment of a broadband (at least a wider band) service within the VHF band. While this technology may prove to offer some future potential, at this time it is a single technology research focus area. This key limitation makes it difficult to lend it credibility as an obvious contender for future A-G communications within the Air Traffic Control (ATC) environment.

Some key areas of concern of this concept include:

- MC-CDMA may work well for the forward link but it is not clear how effective this would be for a return link environment (air-ground) with multiple users contending for common resources

- MC-CDMA provides characteristics that might support coexistence in the VHF band, but it is not clear what advantages this technology would provide in the DME or MLS bands.

- The maximum return link bandwidth using an omni aircraft antenna is governed by the laws of physics and will require either extremely high EIRP or very aggressive ground antenna technology to achieve the stated targets (comparing with VDLm2 – increasing the frequency 8-fold to move into the DME band requires an 8-fold increase in EIRP or receiver directivity just to maintain equivalent data rates and link margin).

2.5.5 P-25

P-25 is a very promising public safety standard developed over the past several years and is under consideration for a nationwide deployment in the US. P-25 has the potential to be very effective in providing voice and narrowband data services but the system has limited range and would need to be suitably modified.

Because P-25 has been developed for public safety applications, it is anticipated that it would be feasible to achieved certification/approval for such a system. Likewise, the fact the P-25 is based upon IP technology supports the long term MCNA network architecture.

2.5.6 P-34

P-34 can effectively be considered as a wideband data extension to the P-25 system. The P-34 concept introduces similar issues as 3-G and B-VHF regarding the question of what return link data rates are intended and whether this will require directional antennas on the aircraft. The wide array of supported physical layer waveforms should provide P-34 the flexibility to offer differing data rates based upon range of the aircraft. This would allow P-34 to provide impressive data rates in the airport domain, moderate data rates in the terminal domain and nominal data rates in the en-route domain. Obviously the data rates achieved could always be enhanced with directional antennas on the aircraft with the associated costs.

Like P-25, since P-34 has been developed for public safety applications, it is anticipated that it would be feasible to achieved certification/approval for such a system. Likewise, the fact the P-34 is based upon IP technology supports the long term MCNA vision.

2.5.7 Future Air-Air System

This is a placeholder to capture requirements for a future system that provides support for air-air communications services.

2.6 Airport Communication Systems

The radio propagation range of many commercial wireless telecommunications systems are limited in comparison with the ranges required for aviation applications. However, many aviation communication service needs are specific to airport surface and terminal domains. As such, communications systems that provide higher data rates and a wider range of services would be applicable for use in these domains. Although many aspects of these communications services will not be available during all phases of flights, operational concepts exist that can take advantage of these enhanced capabilities while aircraft or other mobile vehicles are either at or near an airport.

A unique consideration with airport communication system cost analysis is the estimate of the number of airports that should be equipped to support these services. Sixty-eight (68) airports account for ninety percent (90%) of passenger enplanements and 131 airports account for ninety-seven percent (97%). From a cost benefit perspective, it is much easier to justify investment at the most heavily trafficked airports. However, the usefulness of such a service to an individual airline is dependant upon the service coverage across the range of airports used by their fleet. It is very likely that the initial deployment of these services will be coupled with adoption by a major airline and be focused toward the major airports (at least the hubs) used by that airline.

2.6.1 Airport Data Link (ADL)

Aside from details of the MC-CDMA modulation technique proposed, detailed technical information about aspects of the ADL system is difficult to obtain[4] [8]. Generally, it appears that the ADL research effort is tightly coupled with the B-VHF research and is similarly focused on MC-CDMA technology. Given the wide selection of commercially standardized alternatives, it is unclear whether or not ADL is likely to achieve much traction as a candidate link in this domain.

2.6.2 IEEE 802.11

A version of the 802.11 protocol is used by some airlines today in a service called Gatelink to provide wireless access to aircraft at data rates in the range of 1-2Mbps. These systems operate in the Industrial, Scientific and Medical (ISM) band and are therefore subject to interference from other users in this unregulated spectrum. Nevertheless, this service has proven useful for support of less critical datalink

---

[4] Some information about the proposed modulation scheme is provided at http://www.dlr.de/Tarmac/tarmac_dl/tarmac_adl_en.html

applications and is receiving growing acceptance by the airlines. However, the domain of operation of this system is limited to the gates since the link range is limited to a few hundred meters.

2.6.3 IEEE 802.16

This member of the 802.XX family shows the greatest promise as a link protocol for airport communications. With a range of 50km, QoS support, voice support and mobility support up to 120km/hr, 802.16 can support a wide range of communication service classes to aircraft. Furthermore, the 802.XX family supports a wide range of layered network protocols. However, the primary focus of these datalink protocols has been interoperability with IP.

This datalink protocol is specified for operation over a range of frequencies from 2-11GHz. This allows operation in the MLS band (but not the DME band) and therefore could support life safety services. These protocols have not been certified / approved however they are based upon a thoroughly defined commercial standard which will at least simplify the approval process.

2.6.4 IEEE 802.20

The 802.20 protocol specification is envisioned to be the emerged combined wireless technology that is composed of 802.16 and 3G. It envisions utilizing 3G core networks with 802.xx standards. This member of the 802.XX family is less mature and supports higher mobility speeds but a smaller range. One notable difference is that 802.20 is specified for operation at frequencies below 3.5GHz. This suggests a potential for operation within the DME band that does not exist for 802.16. Other than this spectrum consideration, 802.20 appears to be a less mature variant of 802.16.

2.6.5 TETRA I/II

The TETRA systems really lack sufficient range to provide services other than in the airport domain. TETRA I provides mostly voice and the maturity of TETRA II is very limited. Therefore, this alternative is considered significantly less attractive than the alternatives described. These observations reflect the results from the FCS technology pre-screening.

2.7 Spectrum Considerations

Because of the spectrum congestion and constraints in VHF, many of the new communication links under consideration are within other bands. The two most popular choices for new ATS and AOC communications links are the DME band and the MLS band.

DME

- Unused portions of 960 – 1024 MHz
    - 1 MHz channels
- Interferers
    - Mode-A/C/S & IFF (1030 & 1090)
    - Link-16: JTIDS / MIDS (969 – 1206 MHz)[5]
    - GPS L5
    - UAT
    - TCAS

MLS

- The upper MLS band (5091 – 5150 MHz) is on the WRC2007 agenda for consideration of redesignation for AM(R)S purposes.
- 802.16 supports both FDD and TDD operation.
- MLS use is growing in UK (and some of Europe) and by the United States Department of Defense (USDOD). However this current use is within the lower MLS band. Therefore, limiting AM(R)S use within the upper MLS band would generally relieve these concerns.

In general, the VHF band is very congested with analog voice users. While datalink is purported to relieve VHF congestion by relaxing the need for voice, the primary factor that will reduce VHF spectrum congestion is to change operational concepts so that controllers can handle more aircraft simultaneously. Datalink may reduce the voice activity per channel by eliminating the need for many routine exchanges. However, if the requirement persists to provide a VHF channel for each controller, the number of VHF channel allocations is proportional to the number of controllers and consequently to the number of aircraft operating simultaneously within the NAS.

A final spectrum consideration is the Aeronautical Mobile Satellite Services (AMSS) band. This band is currently used to provide satellite services but recent rulings within the FCC regarding Ancillary Terrestrial Communications allows satellite service providers to also offer terrestrial communication services within their designated spectrum allocations. This introduces the possibility for a common avionics suite that provides communication services via satellite in Oceanic, remote and En-route domains and via terrestrial transponder for gate, surface and terminal airspace. Further study is

[5] A recent MOU will phase out JTIDS/MIDS usage by 2015 [need to provide reference for this]

required to understand the limitation of ATC use and potential for applicability towards MCNA.

3 MCNA NETWORK ARCHITECTURE

One key aspect of the aviation communications environment that greatly complicates the MCNA network architecture is the simultaneous existence of three networking protocols: ACARS, ATN/Connection Less Network Protocol (CLNP) and IP. ACARS is currently the most prevalent for ATS datalink but plans are currently being implemented to supplant ACARS with ATN/CLNP. Furthermore, the industry generally acknowledges that, in the end state, network communications will transition to IP. Specifically, IP communications has been adopted as the foundation for SWIM information transport [7, 11] and ICAO WG-N will soon begin developing SARPs for terrestrial IP data transport with further plans to extend this effort to A-G IP data transport pending a successful feasibility study.

To decompose the discussion of the MCNA network architecture, the architectures of each of these internetworking protocols will by described separately followed by opportunities for inter-working between these networks. The IP-based solution is addressed both from a near term perspective and a long term perspective to provide for consideration of how IP could be reasonably introduced into the ATS environment in the near term while some key protocol extension are still under development.

3.1 MCNA Context and Relationship with SWIM

Prior to a detailed discussion of MCNA network architecture issues, it is useful to describe the context of MCNA particularly as it relates to the System Wide Information Management (SWIM) Architecture [7, 11]. The SWIM architecture depicts the relationship between SWIM, Common Data Transport (CDT) and the supported applications as concentric rings (Figure 5).

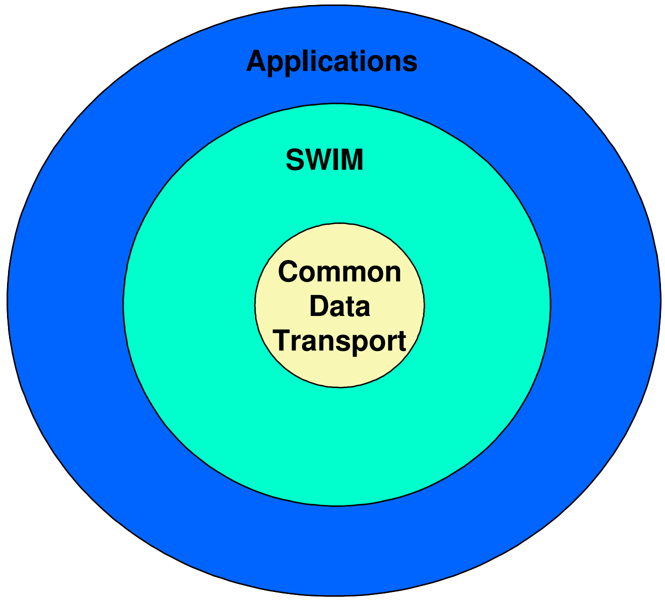

Figure 5 SWIM Context Diagram

In order to support this simplified notional view, the CDT has been defined as the ground-ground networking that supports SWIM. With the introduction of an MCNA, the CDT includes the air-ground networking to support SWIM and eventually even some air-air networking. The scope of MCNA extends beyond support for SWIM services, consequently, the context diagram becomes much more complex (Figure 6). Since the MCNA also supports applications and operator communications that are not SWIM enabled (i.e. voice communications), the scope of SWIM cannot fully envelop MCNA. To help support this view, the notion of CDT is replaced with terrestrial voice & data transport. Therefore, the superset of terrestrial data transport and MCNA represents all ground-ground, air-ground and air-air communication capabilities. The interface between applications and this superset of communication capabilities is often SWIM-enabled but occasionally the interface is direct. This enhanced context diagram (Figure 6) depicts the vision states of both SWIM and MCNA. Transition states would reflect a smaller fraction of SWIM and MCNA deployment.

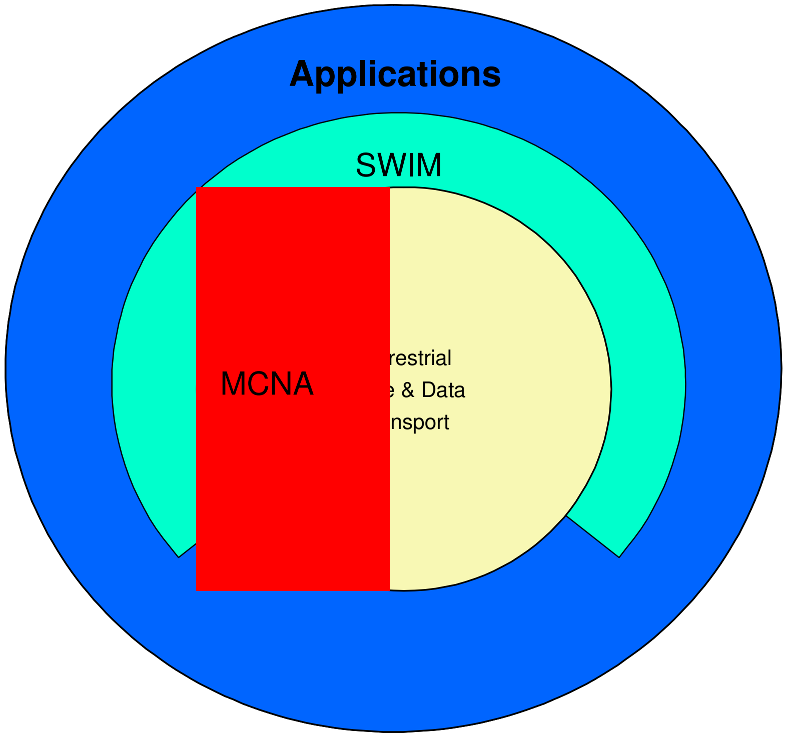

Figure 6 MCNA Context Diagram

3.1.1 SWIM Reference Architecture and Implementation Options

In the SWIM reference model (Figure 7), an application can be Legacy, meaning that the application is not inherently SWIM enabled or Native, meaning that the application is inherently SWIM enabled. Application Adapters (Ad) are used to interface between SWIM and Legacy Applications (LA) and SWIM Shared Services (S^3). SWIM shared services can either be stand alone services such as: registry, directory, naming, messaging, security or client interfaces to these stand alone services. The Common Data Transport (CDT) provides the networking infrastructure to interconnect the various SWIM elements.

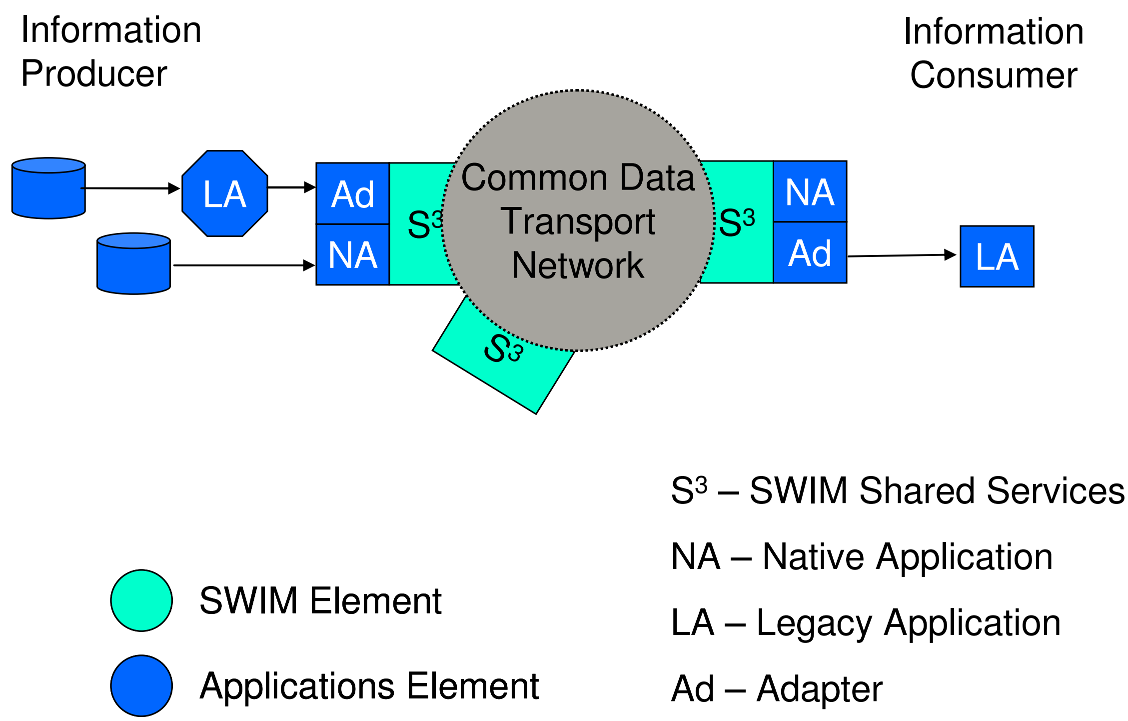

Figure 7 SWIM Reference Architecture

These elements can be combined in a variety of configurations depending upon the needs of the particular application requiring integration into the SWIM (Figure 8). Native SWIM applications have a single configuration with both the application and the S^3 integrated. However, the adaptation of legacy applications for SWIM support can be achieved through numerous configurations. These configurations vary based upon packaging, with the following options:

- LA separate from Ad and S^3 integrated
- LA and Ad integrated and S^3 separate
- LA, Ad and S^3 integrated
- LA, Ad and S^3 each separate

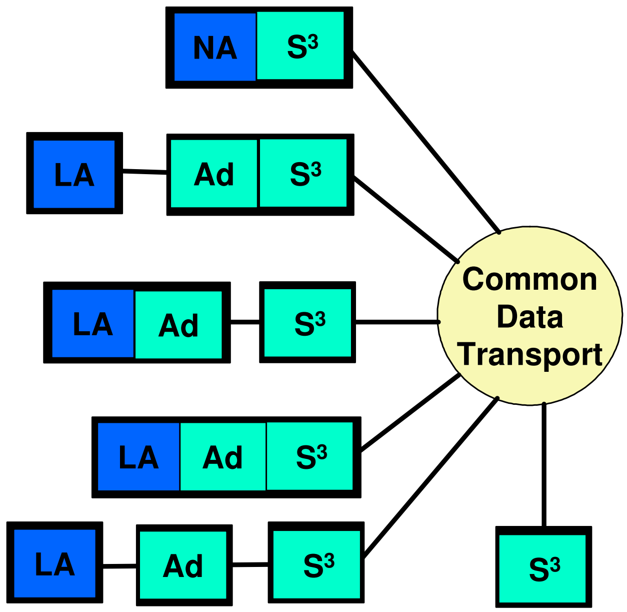

Figure 8 SWIM Configuration Alternatives

3.1.2 MCNA Scope

Given this context on the SWIM architecture, the possible mechanisms for extension of the SWIM to the aircraft via MCNA are investigated. However, before delving into this topic, it is first important to clarify the intended scope of MCNA with respect to SWIM. Figure 9 provides an illustration of the scope of MCNA when it provides CDT to SWIM.

MCNA includes:

- the air-ground links
- the modem/radios in the aircraft
- the airborne networks (ACARS, ATN/CLNP and IP as applicable)
    - routers
    - LAN
    - firewalls
- the ground transceivers
- the terrestrial networks (ACARS, ATN/CLNP and IP DSP networks as used to transport air-ground traffic)
    - router
    - LAN
    - firewalls

- Network Operations Control Center (NOCC)
- Domain Name Service (or equivalent)

SWIM includes:

- SWIM Enabled Applications (SEA) on the airplane (hosts)
- SWIM Shared Services (S^3) on the airplane
    - Message router
    - Information broker & caching
- SWIM Enabled Applications (SEA) on the ground (hosts)
- SWIM Shared Services (S^3) on the ground
    - Message router

The gateways in both the aircraft and the ground networks that support the tunneling of messages and packets over other networks are considered partially within SWIM and partially within MCNA.

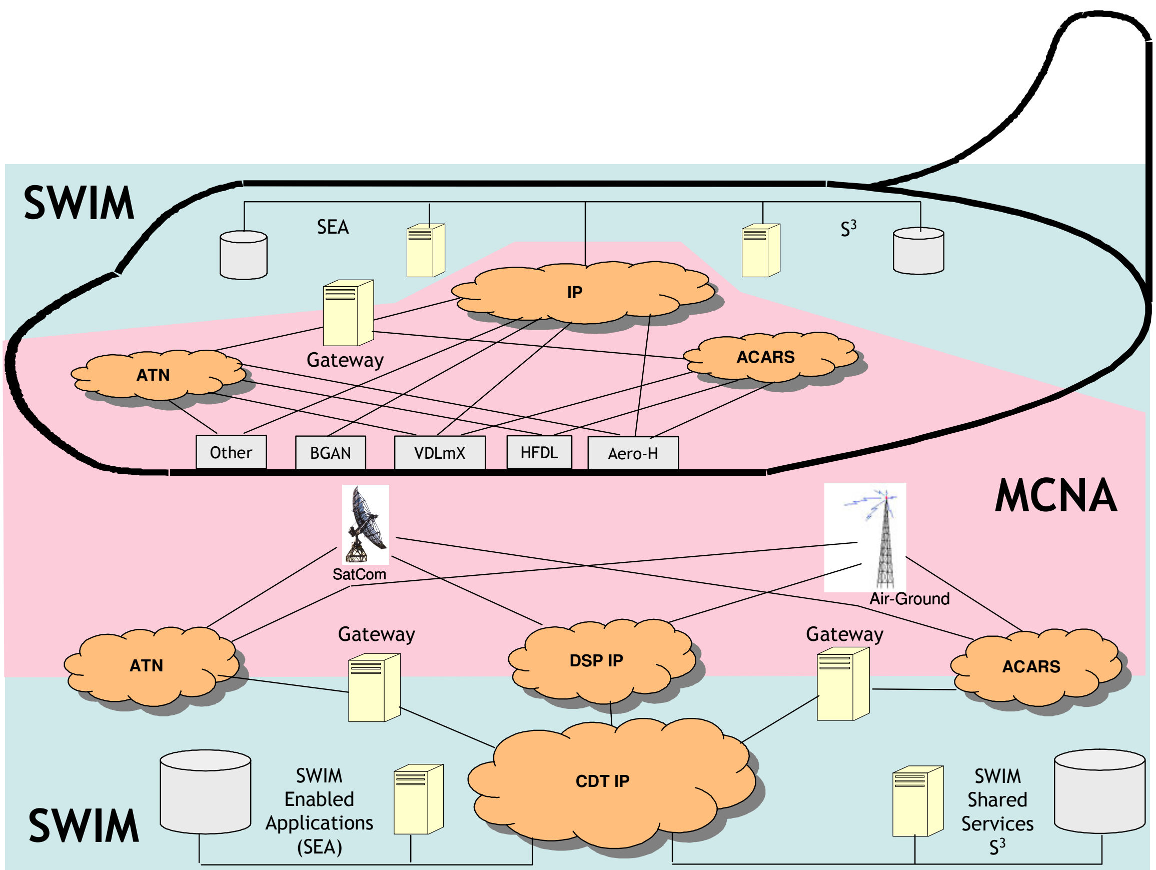

Figure 9 MCNA Scope

3.1.3 MCNA Implementation Options

Three implementation options, Initial, Transition & Vision, have been defined for the extension of SWIM to the aircraft via MCNA (Figure 10). These options outline a progression of MCNA deployment similar to an MCNA transition plan. However, it should be noted that at a given time, an aircraft might implement multiple options simultaneously in support of various applications.

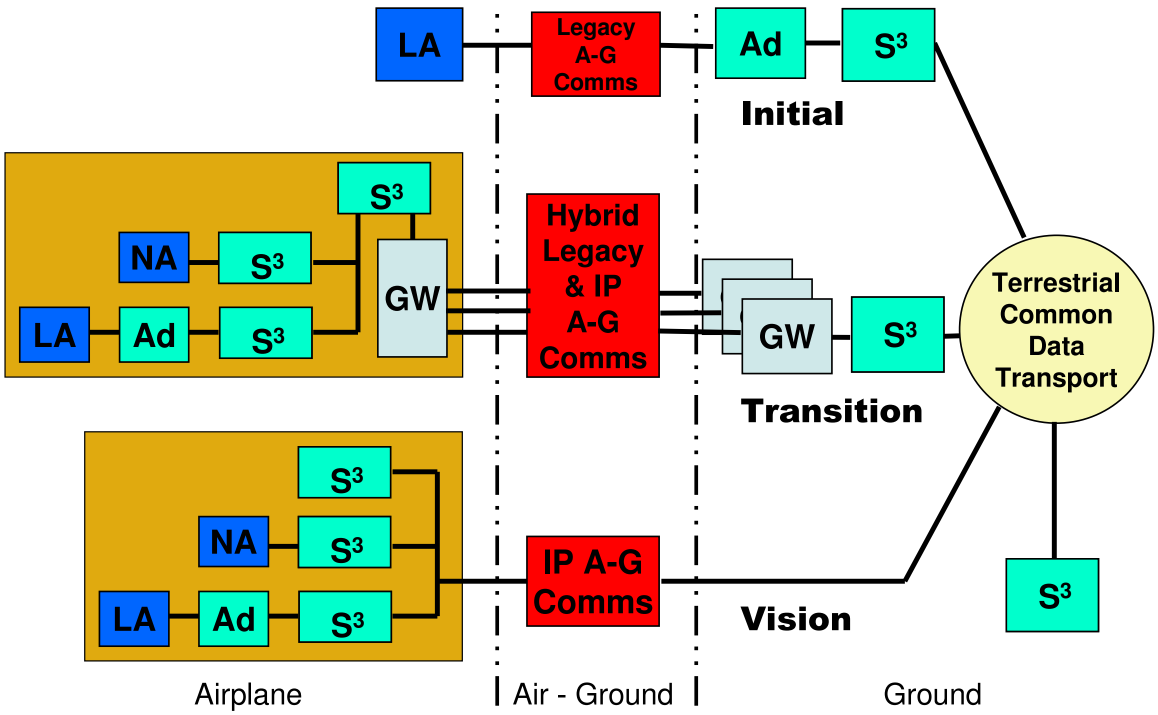

Figure 10 Implementation Options for Extending the SWIM to the Aircraft Using MCNA

3.1.3.1 Initial

The initial and simplest implementation option limits the scope of SWIM to the ground. A legacy aircraft application uses legacy air-ground communications to exchange data with a SWIM enabled application that receives aircraft information and publishes that information into the SWIM. It can also subscribe to SWIM information and forward the subscribed information to the aircraft. This implementation option is the most rudimentary and likely to be the first option to be implemented.

Some examples of potential services that might use this implementation options are listed below:

- Broadcast Services – A SWIM enabled ground application aggregates location specific data through subscriptions to SWIM information services. This application converts the format of this information and generates a broadcast stream over legacy links such as UAT, 1090ES or VDL-B.

- Meteorological Data Collection and Reporting System (MDCRS) – Weather measurements and enhanced weather measurements are sent via ACARS to a SWIM enabled application that publishes the data into SWIM. Multiple applications are able to subscribe to this common information source to facilitate ubiquitous access to this valuable information.

- Out, Off, On, In (OOOI) – Aircraft state information is sent via ACARS to a SWIM enabled adapter that publishes the data into SWIM. The AOC subscribes to this data for operations control purposes, but other ATM applications, such as Traffic Flow Management – Modernization (TFM-M) also subscribe to the same information service to acquire more precise aircraft state information for traffic flow planning purposes.

3.1.3.2 Vision

The vision implementation option is described next because it represents the vision state of MCNA extension of the SWIM and the most elegant architecture. In this architecture, IP-based A-G communications are available that support all of the required functions and capabilities necessary to extend the CDT to the aircraft. The vision state for the MCNA is that it provides the quality of service and required communications performance for safety critical ATS and AOC services, and encompasses the capability to provide seamless AAC and APC services as well. Aircraft applications are either developed natively to be SWIM enabled or interface with the SWIM via an Adapter. This option, as would be expected, is very similar to the SWIM implementation options. However, one key difference is the inclusion of the additional SWIM shared services element. While not a mandatory architectural component, it is anticipated that the bandwidth restriction inherent in A-G communications will mandate the need to provide a subset of SWIM services local to the aircraft domain.

The concept of use is that an on-board SWIM broker would cache static and less dynamic information and provide this cached information local to the aircraft without the need to consume air-ground bandwidth. This information might be loaded manually during aircraft maintenance (such as aeronautical charts), download via a higher bandwidth airport network or received via en-route data broadcast.

3.1.3.3 Transition

The transitional implementation option is the most complex but represents the range of implementations that will likely be employed during the extended transition period that is anticipated. In this option, ubiquitous A-G IP-based connectivity is not available, and aircraft have varying levels of SWIM-compliant equipage. Instead, an aggregate of links supporting ACARS, ATN/CLNP, near term IP and eventually far term IP networks are available. Since many of these links are not capable of supporting the extension of the CDT to the aircraft, SWIM message routing is employed to extend a subset of SWIM services to the aircraft. In fact, messaging currently represents a significant portion of the information transport within the SWIM architecture. Therefore, selecting the SWIM messaging service for A-G transport offers the extension of a significant subset of SWIM services to the aircraft.

A SWIM compliant message router is placed on the aircraft as part of the SWIM shared services (S3). As with the vision implementation, native applications interface with SWIM directly through this SWIM message routers while legacy applications require an adaptor. The airborne message routers can communicate with terrestrial SWIM message routers over a variety of candidate links. Message gateways are employed on both the aircraft and ground to transport/transform messages between routers over these disparate candidate links. One useful feature of this architecture is that the use of message routing to transport SWIM information eliminates the need for network layer mobility, multihoming and policy based routing. Since message routers exhibit store & forward behavior, mobility can be achieved by rapid reconnection with the message router upon link loss or handover. Message routers exchange information at the application layer. This allows for custom implementations of these message routers to achieve policy-based routing and multihoming objectives. As will be shown more thoroughly in later sections, these features of message routing can be employed to provide IP-based services in the near term.

The following example is provided to help clarify this key transition implementation concept:

> A SWIM enabled application desires access to a SWIM service. A subscription message is formulated and sent to the aircraft message router. At this time, the only available A-G link is via AOA. The aircraft message router establishes a connection to a terrestrial SWIM message router using gateways that embed the message into ACARS packets using the plain-text ACARS message capability. A ground gateway extracts the message, re-encapsulates the message into an IP packet and forwards to the appropriate SWIM message router. The SWIM service subscription message is received and the subscribed information is returned via the inverse pathway (through the ACARS message tunnel).

3.2 Networking Technology Introduction

This section introduces the existing and planned networking technologies suitable for MCNA. ACARS is the predominant technology for ATS datalink and is used in the FANS 1/A system that provides service to thousands of aircraft. ATN, based upon customized OSI protocols, is the next generation ATS datalink technology. However, it has experienced extensive deployment delays and airline resistance. Regardless, ATN deployment is underway in Europe even though the ATN SARPS are still undergoing revision to define additional functionality such as security. IP is the dominant world standard for information technology. As a result, it is slowly gaining acceptance within the aviation community as the likely end-state networking protocol. However, the IP protocol stack has key deficiencies that must be addressed to accommodate the requirements defined for ATN[6][12, 13, 14, 15, 16] such as policy based routing and mulithoming. Given the timing of the standardization efforts to address these deficiencies, intermediate IP-based solutions are also being investigated.

3.2.1 ACARS

The Aeronautical Communications, Addressing and Reporting System (ACARS) was introduced in 1976 and is currently responsible for the majority of A-G aeronautical data communications exchanges. However, by today's standards for digital communications, ACARS is extremely outdated technology. The protocol is character oriented, resulting in poor efficiency, does not offer any message prioritization features, has limited addressing capabilities and provides no security mechanisms. In fact, one can search the internet and find a community of people that monitor ACARS message exchanges and post them on the Internet for anyone to read.[7] Furthermore, ACARS was not developed as a layered communications protocol, which limits interoperability and extensibility.

3.2.2 ATN

The ATN concept was initiated in the early 1990's as a replacement for ACARS. Acknowledging the ACARS shortcomings, a new set of protocols was developed to address these issues and accommodate all of the future communication needs. At the time ATN architectural decisions were made, the Open System Interconnection (OSI) protocol family was the preferred international standard mandated by the International Standards Organization (ISO) and various government authorities. These protocols have since been supplanted by the open Internet Protocol (IP) stack, which is in widespread use in the global Internet. Complicating matters further, ICAO was forced to create a series of proprietary (i.e., nonstandard) extensions to the OSI stack in order for ATN to support aircraft networks.

The combination of divergence with commercial networking technology and the need to develop proprietary modifications to the OSI protocols has resulted in an extended development period (almost 15 years with little actual deployment) and a recent realization that the actual "vision" of the ATN should in fact be pursued using the IP family of protocols. As a result, the scope of projected applicability of ATN/CLNP is constantly diminishing towards a transition capability to help advance datalink adoption and utilization until the next generation aeronautical communication network can be deployed.

[6] It is still not clear that many of these ATN requirements are proper requirements or just design solutions.

[7] The following websites can be used to find such capabilities: http://www.airnavsystems.com/, http://www.acarsonline.co.uk/, http://www.kloth.net/radio/hfdl-monitoring.php.

3.2.3 IP – Near Term

While IP is constantly becoming more generally accepted as the desired protocol for aeronautical communications, ATN/CLNP was able to address a number of key requirements related to high availability mobile communications that the IP community is still working to address. Acknowledging that it may still take several years to properly address all of these network architecture shortcomings, near term consideration for the adoption of IP air-ground networking is being addressed within this study. The general notion is that application layer messaging, could address the mobility shortcomings of IP during the interim while a robust and scalable network layer mobility solution is fully developed.

3.2.4 IP – End State

IP networking is being adopted by almost all commercial, civil and military programs for wireless communication. Third generation cellular (3-G), military mobile ad-hoc networks and public safety communication systems have all adopted IP protocols. Furthermore, the Internet Engineering Task Force (IETF) is actively engaged in multiple research and development efforts to address each of the identified shortcomings of the IP protocols (e.g. mobility, multihoming, policy based routing) as related to the support of aeronautical communications.

For these reasons, there is good reason to be confident that the IP protocol suite will soon be able to accommodate the needs of aeronautical communications. Working groups / protocols such as NeMo, MIPv6 and Multi-6 are actively engaged in solving these key deficiencies. Obviously, these working groups could mimic the solutions developed for ATN/CLNP to address these shortcomings. However, the network engineers that support IETF development activities acknowledge the shortcomings of the ATN/CLNP solutions for mobility and are developing solutions that address the required functionality without introducing these same shortcomings. Upon completion of this effort, the IP protocol suite will prove clearly superior to the modified OSI protocols that currently define the ATN/CLNP.

3.3 Routing

3.3.1 Addressing

Three networking protocols (ACARS, ATN/CLNP & IP) will result in multiple addresses for each aircraft. This introduces an interesting network architecture challenge that must be addressed. While the ACARS and ATN/CLNP addressing schemes are currently defined, an IP addressing scheme must also be proposed. The following table, Table 3, summarizes the key characteristics of network addressing for the four options while the following sub-sections describe these addressing approaches in more detail.

Table 3 Network Addressing Comparison

	ACARS	ATN/CLNP	IP Near Term	IP Far Term
Packets Include Source Address?	Downlink only	Yes	Yes – (Reply To Address)	Yes
Packets Include Destination Address ?	Uplink: Aicraft ID or flight number, Downlink: label & sublabel	Yes	Yes	Yes
Aircraft ID	Aircraft registration or Flight ID	24-bit ICAO aircraft address	Plan to use 24-bit ICAO address	Configurable with interface ID, plan to use 24-bit ICAO address
What Addresses Represent	Aircraft, labels used to get to individual applications	Packet Router	Application	Interface

3.3.1.1 ACARS [5]

Addressing in ACARS is limited to the aircraft identification mark. Air-to-ground (downlink) messages include the aircraft registration mark in ISO-5 encoding and a flight identifier embedded in the message text field. The aircraft registration mark is right justified and preceded by periods (".") to always be seven (7) characters in length. The flight identifier consists of a period ("."), a two (2) character airline ID and a four (4) character flight number. Business and commuter aircraft use an aircraft address instead of the registration mark.

Ground-to-air (uplink) messages include either an aircraft identification address or a flight identifier in the same format as for downlink messages. ATS message must use an aircraft ID address for uplink messages.

Addressing in ACARS is also achieved using:

- Labels
- Sub-labels
- Supplementary addresses (in the message text of downlinks)

- o DSP Identity (in the mode field)
- o Site Address

In general, the addressing architecture of ACARS is a severe limitation and a key reason for the original migration towards ATN/CLNP.

3.3.1.2 ATN/CLNP [8][7]

The ATN/CLNP address consists of two main sections, the first of which is used for routing and administrative information, and the second of which uniquely identifies the addressed host (Figure 11). The International Standards Organization (ISO) assigns the Initial Domain Part (IDP). Any organization requesting an OSI address space first registers with the ISO and receives an IDP to support area routing. The remaining portion of the address is administered by the requesting organization, in this case ICAO. The ATN/CLNP address portion administered by ICAO is defined somewhat[9] more completely in ICAO Document 9705, Sub-Volume 5, otherwise known as the SARPs.

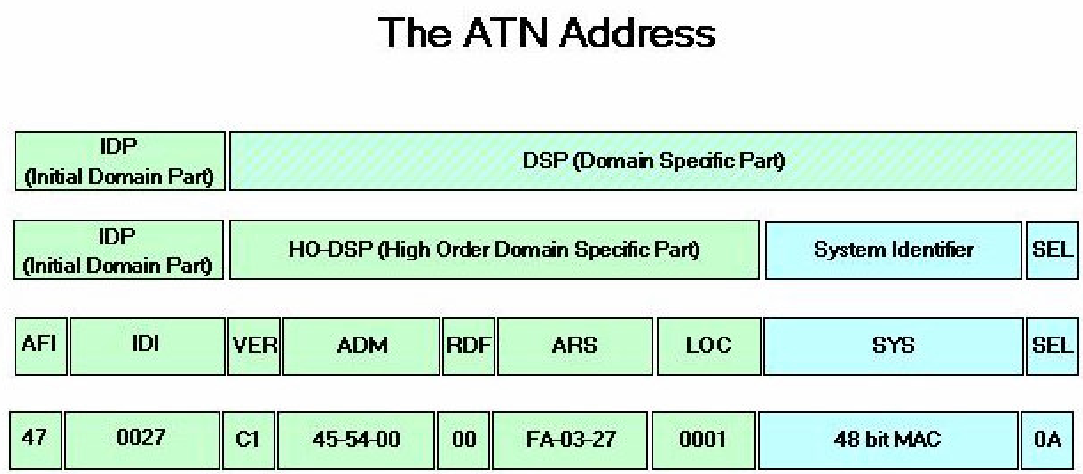

Figure 11 The ATN/CLNP Address

Authority Format Identifier (AFI) – 1 octet, Binary Coded Decimal (BCD).

- o Allocated by the ISO. All ATN/CLNP addresses have an AFI value of 47 decimal.

---

[8] This section was adapted from a similar section in the GCNSS-I CIN Architecture Document (as referenced).

[9] The term "somewhat" is used because the actual administration of the address space is still being architected and there are at least two competing schemas within ICAO.

Initial Domain Identifier (IDI) – 3 octets, BCD.

- Allocated by the ISO
- All ATN/CLNP addresses have an IDI value of 0027 decimal.

Version (VER) – 1 octet, binary-encoded.

- Used to partition the ATN into subordinate domains.
- ATN allows four values:
    - x01 - Fixed Aeronautical Industry Service Communication (AINSC) (Commercial)
    - x41 – Mobile AINSC (Commercial)
    - x81 – Fixed Air Traffic Service Communication (ATSC) (GA)
    - xC1 - Mobile ATSC (GA)

Administration (ADM) – 3 octets, either IA-5 encoded alphabetic or IA-5 encoded hex/alpha combination.

- ADM is used to further subdivide ATN domains.
- For fixed hosts, either a hex representation, translated using IA-5 encoding, of the 3-letter designation for a domain (for example EUR is encoded as 45-55-52), a hex encoding of the three letter ISO3166 Country Code (for example GBR = 47-42-52), or a fixed code as supplied by ICAO as follows:
    - x80 – Africa
    - x81 – Asia
    - x82 – Africa
    - x83 – Caribbean
    - x84 – Europe
    - x85 – North America
    - x86 – Middle East
    - x87 – North Atlantic
    - x88 – South America

The corresponding ICAO region assigns the remaining two octets. If the address is mobile (as identified by the VER field), the field is entirely designated by the airline for commercial aircraft or the country of registration of the GA aircraft. This field appears to be quite arbitrary, and highly dependent upon a series of “recommendations” by the ICAO.

Routing Domain Format (RDF) – 1 octet, binary-encoded hexadecimal.

- Not used and filled with zeroes [x00].

Administrative Range Selector (ARS) – 3 octets, unsigned binary-encoded hexadecimal.

- In fixed hosts, each state or organization chooses their own usage for this field, and can use one, two or all three octets.
- Unused octets are zero-padded.
- Mobile hosts use the 24-bit ICAO Aircraft address in this field. Some committees within the ICAO are proposing a sub-division of the field into three sections: Network ID, Network Group, and Domain ID.

Location (LOC) – 2 octets, binary-encoded hexadecimal.

- Used for “sub-netting” administrative ranges, for example if an aircraft had more than one network on board, the administrator for that aircraft could assign separate values in this field, creating “routable” subnetworks.
- ICAO has recently proposed subdividing this field into Sub-domain Group and Sub-domain ID

System Identifier (SYS) – 6 octets, binary-encoded hexadecimal.

- ISO actually specifies this as a variable length field, but ATN pegs it at 48 bits.
- Unique host identifier, commonly the 48-bit MAC address of the host, although there is a movement within ICAO to assign numbers without regard to hardware dependencies, in a format similar to IP.

NSAP Selector (SEL) – 1 octet, binary-encoded hexadecimal.

- Used to select among multiple transport layer entities in an end system.
- The SEL field is analogous to TCP/UDP ports.

- Intermediate systems are required to use [x00] in order to forward packets; otherwise this field is application dependent.

3.3.1.3 IP – Near Term

In the near term, it would be desirable to use the same IPv6 addressing as planned for the long term. However, since the near term IP solution relies up message routing, an additional level of addressing is introduced at this application layer. This application layer addressing is more relevant and will be addressed in this section.

Messaging system addressing is somewhat dependant upon the messaging system, however the general trends is towards Web Services (WS) Addressing scheme. WS Addressing uses Universal Resource Identifiers (URI) to identify source and destination nodes. These URI's are statically configured and the system provides sufficient flexibility to allow aircraft to be identified via their ICAO 24-bit address. A possible example of such an URI might be the following:

http://atc.faa.icao/{airline}/{ICAO_address}/application

Since this is an application layer address, it can be assigned statically and does not require changing with the motion of the aircraft. The network address would change as a function of mobility and the DNS servers (or a special messaging system equivalent) would be updated each time a mobile nodes changes network addresses.

IP - End State[10] [7]

Globally unique unicast addresses are based on the IPv6 Aggregatable Global Unicast Address (AGUA) format. ICAO or another suitable international body will obtain Top Level Aggregator (TLA) status with a Regional Internet Registry (RIR) such as American Registry of Internet Numbers (ARIN). At this time, the three existing RIRs cover a service area that spans the entire world, including:

- Europe and the Middle East (RIPE NCC)
- Africa (ARIN & RIPE NCC)
- North America (ARIN)
- Latin America including the Caribbean (ARIN)
- Asia Pacific Network Information Center (APNIC)

Further consideration should be given toward establishing the ICAO or other global organization as an RIR in its own right, becoming a peer of ARIN, RIPE, etc.

[10] This section was adapted (slightly) from a similar section in the GCNSS-I CIN Architecture Document (as referenced).

In any case, ICAO will assign the appropriate organizational IPv6 addresses from its assigned TLA address space. It is assumed that this TLA space will be on the order of a "/24"; that is, the first 24 bits of the 128 bit IPv6 address space is reserved, leaving the remainder available for organization-level addressing. The ultimate size of the address space will be the subject of negotiations within ARIN and the ATM community. Examples of organizations may include:

- Aeronautic Service providers, such as ARINC and SITA
- IATA, representing Major Commercial Air carriers
- National Civil Aviation Authorities, such as FAA.
- National military aviation infrastructures
- A separate system-wide organization for network management and accounting. This address space would be out-of-band, but parallel to the remaining CTN.

Organizations will assign address space to their internal PoPs and PoPs will assign address space to their sites. A point of presence (PoP) is defined to be an entity or region that provides network access for sites. A site is defined to be any physically or logically separate ATM unit that is not a PoP. For mobility purposes, each aircraft is also associated with a site; for example a Delta 767 could be a subnet of a Delta Airlines site.

The current baseline for NAS operation is based on collocation of the PoP structure with major FAA facilities, in which each Air Route Traffic Control Center (ARTCC) is a PoP that services those sites within its geographic area. Obviously, this baseline is subject to change and other organizations will devise their own address sub-architectures.

Figure 12 provides a graphical representation of this hierarchical address management structure. It should be noted that sites will have numerous subnets according to their operational needs. These examples are intended to show a general hierarchy rather than a specific implementation.

Heirarchy	Example 1	Example 2	Example 3
IANA	IANA	IANA	IANA
RIR	ARIN	ARIN	ARIN
TLA	ICAO	ICAO	ICAO
Organization	FAA	IATA	US DoD
PoP	ZLA	Delta Airlines	USAF Europe
Site	LAX	DAL Atlanta	Raamstein
Site Subnets	LAX Subnets	Atlanta AOC	SAR

Figure 12 Address Assignment Hierarchies

Applying the above guidelines to the AGUA format produces the following addressing template, including Top Level Aggregation (TLA) Identifiers (ID), Next Level Aggregation (NLA) IDs and Site Level Aggregation (SLA) IDs (Table 4).

Table 4 IPv6 Address Heirarchy

Specification Field	Size in bits	Prefix	Significance
Format Prefix	3	001	Required Format Prefix
TLA ID	13	0xXXXX	ICAO TLA Identification
NLA ID	13	0xYYYY	Organizational ID
NLA ID	11		POP ID
NLA ID	12		Site ID
SLA ID	12		Site subnets
Interface ID	64	0xZZZZ ZZZZ ZZZZ ZZZZ	EUI-64 Interface ID

This addressing template provides the following maximum values:

- 8192 maximum organizations

- 2048 maximum major POPs for each organization
- 4096 maximum sites serviced by each POP
- 4096 maximum subnets for each site

Although this proposed hierarchy appears somewhat inverted, political considerations may require more addresses at the “organizational” level than would otherwise be necessary. Accordingly, we have “borrowed” some bits from the SLA level to provide an expanded address space at the organizational level.

These constraints lead to a total ATM address space (assuming perfectly efficient address allocation) of well over one billion networks, with each network containing a virtually unlimited number of hosts.

3.3.2 Topology[11] [7]

Topology is the second key consideration for routing architectures. The physical topology of an inter-network is described by the complete set of routers and the networks that interconnect them. Networks also have a logical topology that defines the logical relationships between network entities. The logical topology may be quite different from the underlying physical topology.

Different routing protocols establish a logical topology in different ways. Some routing protocols do not use a logical hierarchy but instead use addressing to segregate specific areas or domains within a given internetworking environment and to establish a logical topology. For such nonhierarchical or “flat” protocols, no manual topology creation is required.

Other protocols require the creation of an explicit hierarchical topology through establishment of a backbone and logical areas. The Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) protocols are examples of routing protocols that use a hierarchical structure. A generic hierarchical network scheme is illustrated in Figure 13.

[11] This section was adapted from a similar section in the GCNSS-I CIN Architecture Document (as referenced).

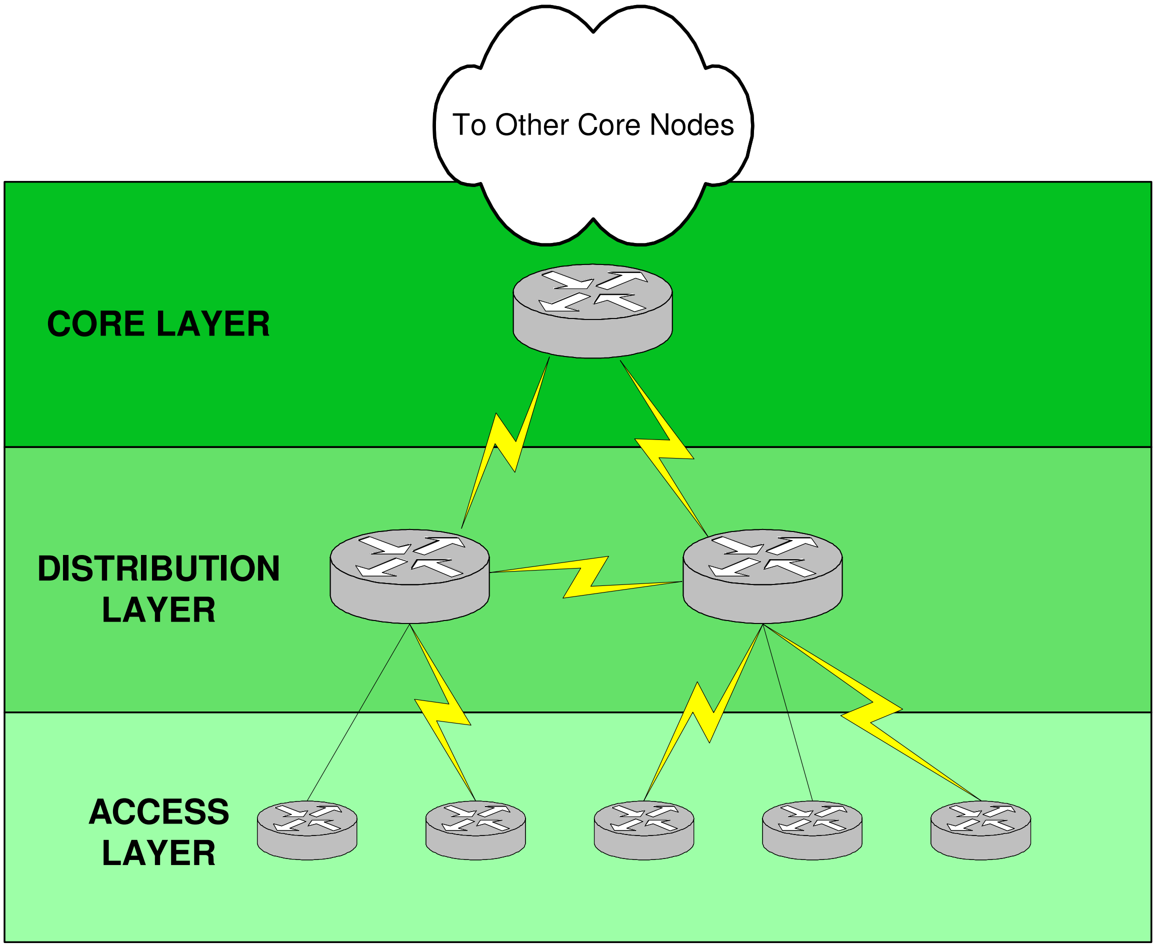

Figure 13 Generic Hierarchical Network Topology

The explicit topology in a hierarchical scheme takes precedence over any topology created through addressing. If a hierarchical routing protocol is used, any assigned addressing topology should reflect this hierarchy. Conversely, if a flat routing protocol is used, address assignments themselves define the topology.

There are two recommended ways to assign addresses in a hierarchical network. The simplest approach is to assign each area (including the backbone) a unique network address. An alternative is to assign address ranges to each area. Areas are logical collections of contiguous networks and hosts, together with the routers having interfaces on any of the included networks. Each area runs a separate copy of the basic routing algorithm and therefore has its own topological database.

Ideally, topology and addressing are closely aligned to maximize addressing and routing efficiency. However, this is unlikely to occur in practice because of mismatches between managerial and physical boundaries. For example, an international service provider could have an address space that appears to emanate from multiple locations, each of which injects addresses into the network core that could otherwise be aggregated.

The topology of each network varies significantly. The selection of a topology defines the scalability and robustness of the resultant network. Table 5 summarizes key aspects of the network topologies while the following sections describe these topologies in further detail.

Table 5 Network Topology Comparison

	ACARS	ATN/CLNP	IP Near Term	IP Far Term
# Routers	1 per Service Provider	2 initially in the NAS	Message router per ground transceiver and one at each facility (as part of SWIM)	Access router per ground station, one core router and at least on distribution router per ARTCC and distribution routers at other major FAA facilities.
Logical Toplogy	No	Possible	No (message), Yes (IP)	Yes
Tiers	Single	Dual (currently planned) with ability to grow	IP – 3 Tier Message – 2 Tier	IP – 3 Tier

3.3.2.1 ACARS

The network topology for ACARS is very simple, each service provider has a single message router. All messages are sent to this router for forwarding to their intended destination. This topology introduces some issues regarding robustness and scalability. In order to increase the reliability or throughput of the system, the performance of this single message router (or message routing function) must be increased. This has historically been an issue regarding message delivery latency. As the demand for ACARS increases or peaks for a short duration, the ability of the existing hardware to process these messages becomes a limiting factor. As a result, poor latency performance has been experienced over the years within the ACARS network.

3.3.2.2 ATN/CLNP [7]

Routing packets through the ATN is accomplished through the use of OSI standard routing procedures. In order to better understand ATN/CLNP routing, it may be useful to define an ATN inter-network. ICAO defines an ATN inter-network as “a set of interconnected Routing Domains (RD), within the global OSI Environment (OSIE). Each such RD shall contain Air Traffic Service Communication (ATSC) and/or Aeronautical Industry Service Communication (AINSC) related Intermediate and End Systems.” The concept of RDs is key to the ATN/CLNP routing scheme. Each domain is to be “unambiguously identifiable”, meaning unique. An RD can be an aircraft, a company, a country or a continent.

Unfortunately, since there is no central administrative function in the ATN other than the recommendations of ICAO, member organizations are free to create and modify RDs at will, leading to significant disorganization within the routing architecture. This disorganization could lead to scalability problems, since it may be difficult to aggregate routes as effectively as with a centrally addressed system such as IP.

Within the larger scope of the ATN, these RDs are confederated into “islands”. The initial implementation of ATN/CLNP within the NAS anticipated requiring only two ATN/CLNP routers.

3.3.2.3 IP – Near Term

In the near term, the IP routing architecture should be similar to that in the end states. However, the extent of the network may be significantly reduced in this timeframe. The message routing architecture would consist of access message routers at each air-ground facility to assist with mobility and multihoming functions plus a set of message routers at the ARTCCs and other major FAA facilities.

3.3.2.4 IP - End State

The IP end state routing topology should align with the FTI architecture and should be represented by the proposed CTN topology defined during GCNSS I [7]. The routing topology is hierarchical as defined previously in Figure 13. Each ARTCC would host both a core router and one or more distribution routers. Additional distribution routers would be located at TRACONs, major airports and other significant FAA facilities. Access routers would be collocated with air-ground communication facilities.

3.4 Mobility [7]

Mobility addresses the need for mobile nodes to initiate and maintain connections while new connections are established and old connections are lost. A key consideration of mobility is the means for a host to initiate communications with a mobile node without current knowledge of the location of that node. Mobility can be solved at multiple layers within the OSI reference model, most commonly the link layer, the network layer and the application layer. Each of these mechanisms will be discussed briefly below followed by a discussion of how mobility is currently addressed by ACARS and ATN/CLNP and the proposed mobility solutions for IP in both the near term and vision state. A summary comparison of mobility techniques is provided in Table 6.

Table 6 Mobility Comparison

	ACARS	ATN/CLNP	IP Near Term	IP Far Term
Link Layer Mobility	Applicable for appropriate datalinks	Much of ATN mobility in NAS planned at link layer	Applicable for SatCom, 802.x, etc	Applicable for SatCom, 802.x, etc
Network Layer Mobility	NA	Supported by IDRP	NA	IPv6 protocols still in development (likely NeMo)
Application Layer Mobility	Mobile message router logs into access message router to delivery/retrieve messages	NA	Mobile message router logs into access message router to delivery/retrieve messages, eliminate Type A / Type B conversion	NA

3.4.1 Link Layer Mobility

Link layer mobility relates to the movement of a mobile node between access points on the same sub-network (Figure 14). An example would be a wireless device moving between 802.11 access points. Link layer mobility is typically accomplished using proprietary protocols in order to achieve more seamless handovers. These mobility events tend to be very quick but happen between access points from the same network attached to the same router. A mobility event between access points on different sub-networks results in the need to update routings tables and possibly network addresses. As such, these mobility events are defined as network layer mobility. A key variable on the timing of a link layer handover is whether link layer security associations are employed and whether these associations can be forwarded or need to be re-established.

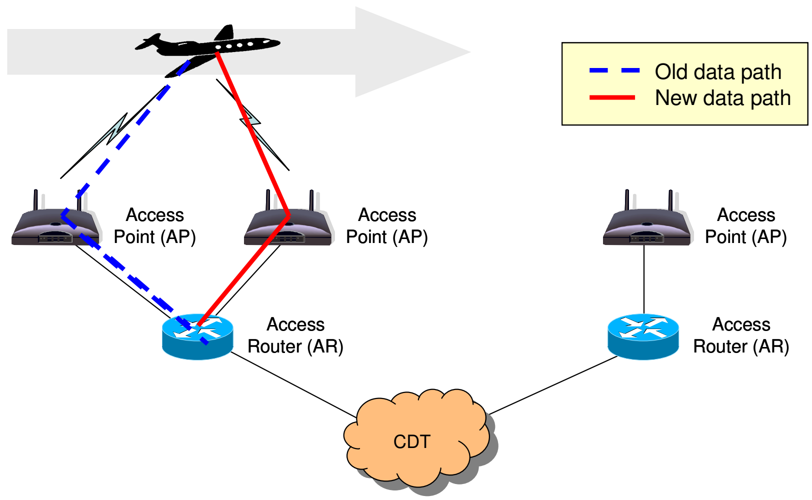

Figure 14 Link Layer Mobility

3.4.2 Network Layer Mobility

Network layer mobility involves the movement of mobile nodes between network access points that are attached to different routers within a network (Figure 15). Network mobility is achieved in one of two ways. The mobile node can either retain its network address or request a new address from next serving router. With the first approach, the routing tables in the network routers must be updated to reflect the new routes for this mobile node. This solution introduces several scalability issues. The latency to stabilize after a mobility event is dependant upon the time necessary to propagate routing table updates across the network. If a large number of mobility event are constantly occurring, the traffic between routers to maintain routing tables could become significant.

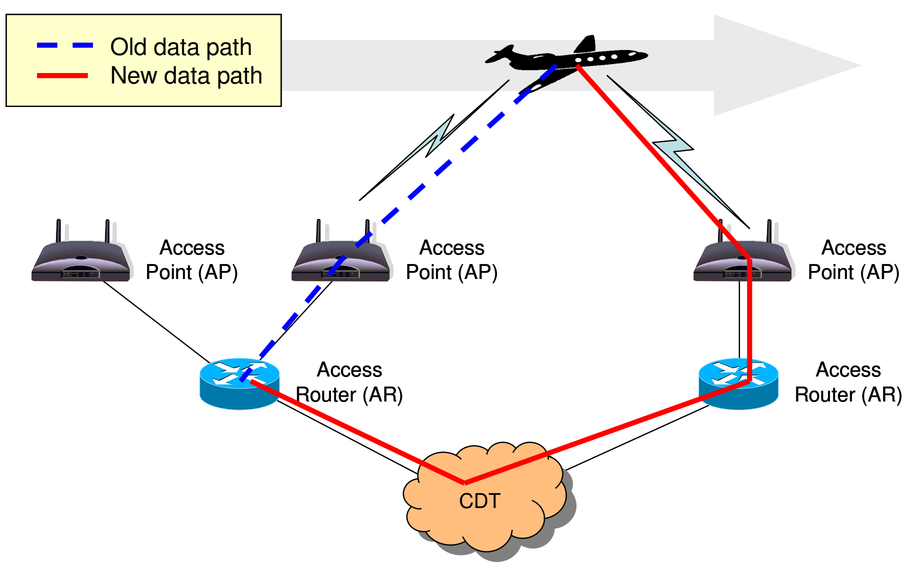

Figure 15 Network Layer Mobility

Alternatively, if nodes are allowed to maintain their network address as they move, it is not possible to maintain a hierarchical routing and addressing topology and each router must manage very large routing tables to identify the next hop for each mobile node in the network. This approach reflects the mobility solution provided by ATN/CLNP using IDRP. It has been argued that since only 10,000 to 20,000 aircraft are anticipated to be airborne at any given time, the routing tables could remain manageable with this mobility approach. However, experience to date has demonstrated that scalability concerns to date with the Link2000+ program have required the modification of the ATN/CLNP router to include a hardware-based Route Processor module to handle the routing table.

The alternative network mobility approach is to rely upon fixed nodes, called Home Agents, to act as relay stations for mobile nodes. The mobile node maintains a "Care of Address" (CoA) that is routed to its serving home agent. As the mobile host moves, it is assigned new IP addresses that are consistent with the network addressing topology. The mobile host communicates these network address updates to the home agent so that future packets can be properly encapsulated and forwarded to the mobile host. In many ways this concept is similar to mail forwarding in the postal system. This is the preferred mobility approach in IP. This mobility solution is much more scalable but introduces some latency problems since packets have to be routed through an intermediate host. The Home Agent has also been identified as a single point of failure with this mobility solution. As a point of reference, this mobility solution was selected for the Cellular Digital Packet Data (CDPD) network and successfully served ~10-20k mobile nodes nation-wide mostly for public safety applications [27].

3.4.3 Application Layer Mobility

A Message Transport Service (MTS) provides application layer routing using store and forward message routers (Figure 16). Mobile hosts are required to log into a message router to download their messages and send any new messages. If the mobile host loses a link, a new link is established and the host reconnects with the message router. Since the message router stores messages until they can be forwarded to their next hop, no messages are lost during the link outage. A very common example of application layer mobility is email. Simple Mail Transport Protocol (SMTP) is used between email gateways (message routers) and Post Office Protocol Version 3 (POP3) or equivalent is used between mobile hosts and the service email gateway. This is the current means of mobility for ACARS and the proposed near term mobility solution for IP.

This mobility approach is limited to forms of information exchange that can be accommodated through messaging. For example, messaging is not an appropriate mechanism for voice, video or other forms of real-time peer-peer information exchange but is very applicable for the transport CPDLC, ADS and FIS messages. Therefore, consideration must be given to the type of information exchange needed in the near term. The primary communication service to be supported by ATN is CPDLC which is a messaging based service. As such, it is not clear that such a complex mobility scheme, as defined by the ATN SARPS, is in fact necessary. This consideration was accounted for when defining near term IP mobility requirements. Furthermore, messages can be exchanged over IP, CLNP or ACARS based links. As such, the application layer mobility solution provides mobility across sub-networks of disparate network protocols.

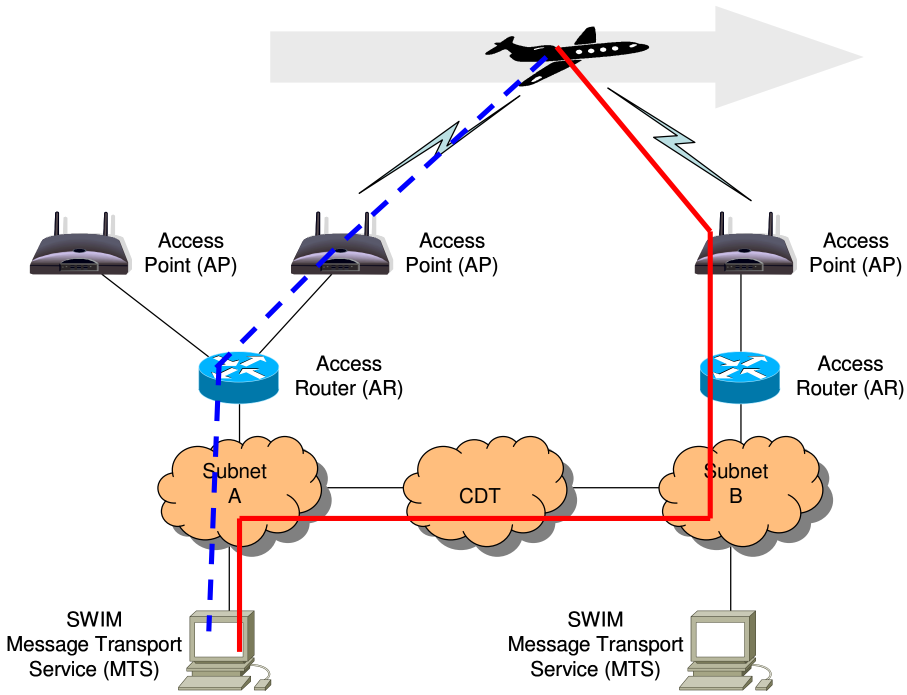

Figure 16 Application Layer Mobility

3.4.4 ACARS [5]

ACARS mobility is achieved through message routing. The aircraft must initiate a datalink session by logging onto the Datalink Service Provider (DSP) ACARS network. ACARS message routing is divided into an air-ground portion and a ground-ground portion. The air-ground messaging uses Type-A messages and is somewhat archaic. Ground-ground messaging is based upon Type-B messages and has evolved to IBM's MQSeries messaging system which is relatively state of the art. A Type-A to Type-B message conversion function is required between the two systems.

Another aspect of ACARS mobility has to do with the operation mode. This discussion is specific to ACARS over VDL. In category A operation, a downlink message is sent to all service provider ground stations which receive the message and forwarded to the message processor. In this operation mode, multiple copies of the message may be received and it becomes the responsibility of the message processor to handle duplicate messages. In category B operation, downlink message are addressed to a particular DSP ground station.

3.4.5 ATN/CLNP [7]

ATN addresses mobility both at the link layer and the network layer. AVLC addresses mobility between ground stations that are connected to the same ATN/CLNP router. When an aircraft moves between ground stations that are attached to different ATN/CLNP routers, the Inter Domain Routing Protocol (IDRP) that has been customized to accommodate the unique requirements of ATN, manages the mobility event by distributing new route information through the network. The near term planned ATN topology has very few routers (e.g. only 2 planned in the NAS) and therefore relegates most of the mobility to the link layer. This network design helps address the scalability issue by employing fewer complex routers that can accommodate very large routing tables.

3.4.6 IP – Near Term

It is proposed that mobility for IP air-ground networks can be addressed in the near term by adopting a mobility solution that is an evolution of that used for ACARS. The general notion is to extend the evolved ACARS ground-ground messaging architecture to also include air-ground applications. Ideally, Type-B (or equivalent) message would be exchanged between the airborne message router and ground applications. However, this would require a message transformation function on the aircraft to convert Type-B messages into the Type-A format expected by the legacy applications. This functionality would in fact represent a portion of the SWIM adapter element described previously.

3.4.7 IP - End State [7]

In the vision states, IP version 6 (IPv6) with mobile IP version 6 (MIPv6) and network mobility (NeMo) extensions would accommodate the mobility requirements. This solution would allow aircraft to maintain a static Care of Address (CoA) that is used by others to address communications to the aircraft. As discussed previously, this would enable the IP network to maintain a route aggregatable[12] network/addressing topology that provides the robustness and scalability seen today in the global internet. The home agent (HA) function would likely be located at the AOC. Since the HA has been identified as a potential single point of failure, a special HA implementation would likely be developed to assure the required service availability.

3.5 Multihoming [7]

Multihoming is an aspect of routing/mobility that accounts for multiple simultaneous connection from a host or router to the network. For MCNA, we are considering multiple simultaneous connections from the aircraft (via air-ground sub-networks) to the

[12] Aggregatable routes allow routers to forward packets within an address range to a particular egress interface. This reduces memory and processing requirements on the router rather than having t look up each address using a hash table or equivalent.

terrestrial network. Multihoming is not in fact a requirement but a solution proposed by the ATN to address the issue of maintaining high service availability in a mobile environment. The notion being that high availability would require multiple simultaneous links that are transient in nature and consequently require an ability to rapidly and seamlessly move flows between these links to provide "make before break" handoffs.

Given this background, it is evident that the requirement for this capability needs to be revisited. While MCNA shares the philosophy that the network architecture should address multiple links, it is not clear that these links must be used simultaneously by the same aircraft sub-network in all cases. Given the notion of communication service classes and level, defined in the MCNA Requirements Report [26], the need for a true multihoming capability is driven by the latency requirements (specifically the transaction Expiration Time (ET) requirement). Many of the communication service classes and levels are not likely to drive a requirement for simultaneous connections if the system is able to establish links within a reasonable time. Because the need for this functionality is strongly correlated with the ET requirement, it becomes imperative to re-evaluate the ET sub-allocation process to determine if a larger latency allocation can be provided to the communication services than is currently documented. Furthermore, depending upon the availability of the individual communication systems under consideration, it can be argued that the time for the router to establish a backup link would not even fall within the ET allocation but rather be considered as action taken to establish an alternate means of communication.

Classically, multihoming is concerned with multiple network connections to the same network. The aviation environment must also consider multiple simultaneous heterogeneous network connections (ACARS, ATN/CLNP & IP). In many ways this simplifies the problems, however new issues will inevitably arise. Also, the aircraft may have multiple simultaneous air-ground sub-network connections via similar networks as well as dissimilar networks.

Table 7 summarizes key comparative aspects of the multihoming architecture while the following sections describe these architectural characteristics in further detail. Comparison parameters within this table include:

- The element responsible for selecting which link to send a downlink (A-G) communication
- The element responsible for selecting which link to send an uplink (G-A) communication
- The network protocol(s) employed to achieve Multihoming

Table 7 Multihoming Comparison

	ACARS	**ATN/CLNP**	**IP Near Term**	**IP Far Term**

A-G Link Selection Element	MU	CMU	Airborne message router or gateway	CMU/Airborne IP Router
G-A Link Selection Element	DSP	ATN/CLNP Router	Terrestrial message router or gateway	TBD (based upon the outcome of Multi-6 effort), possibly the Home Agent
Protocol	Proprietary	IDRP (w/ customizations)	SCTP or proprietary messaging based	TBD (based upon the outcome of the Multi-6 effort)

3.5.1 ACARS [5]

In ACARS, multihoming is provided through custom functionality in the Management Unit / Communication Management Unit (MU/CMU) and the DSP. Since ACARS does not treat the disparate A-G link as parts of a greater network with a distributed routing function, the complexity to support multihoming is not as severe. For datalink exchanges that are air-initiated, the MU/CMU selects the desired medium based upon link availability and other criteria (discussed further in the policy-based routing section). For ground initiated messages, the DSP selects from the available links (as registered during logon and/or updated via maintenance) and forwards the message based upon the airline policy as defined in the DSP. Return messages are delivered based upon the policy of the sending node (MU/CMU or DSP) regardless of the link from which the originating message was received. This would allow a message to be sent over a given link type to be returned over a different link type due to link failure following the original message delivery.

3.5.2 ATN/CLNP [12, 13, 14, 15, 16]

Multihoming is a capability that is supported by the proprietary IDRP variant used for the ATN. The establishment of additional air-ground connections is registered in both the airborne ATN/CLNP routers and the terrestrial ATN/CLNP network (routers) as an additional route to the aircraft. Similarly, lost air-ground connections would be detected by the airborne and service ground routers and forwarded through the terrestrial network as applicable. Routing policy (as described in the next section) is defined within the airborne ATN/CLNP router and distributed through the ATN network as part of the router advertisement and distribution function.

3.5.3 IP – Near Term

The proposed solution for near term IP multihoming is still very much in the formative stages. Two concepts were briefly investigated, however, the scope of this effort limited the level of detail that could be pursued.

The first solution involves the extension of the message routing function to include provisions to address multihoming. The airborne message router establishes redundant message channels over each available A-G sub-network from each service provider. A message router must be placed within each service provider's sub-network to allow the desired level of granularity of route selection for multihoming support. The redundant message channels are differentiated by the next hop message router located in each of the sub-networks. Management of multiple simultaneous links between the aircraft and the same datalink sub-network would be managed at Layer-2 as is accomplished currently for ATN.

The alternative proposal is to employ Stream Control Transport Protocol (SCTP) between the gateways (as shown in the second implementation option in Figure 10) [29, 30]]. Locating this functionality into these custom gateways, allows the use of COTS technology for the message router. However, this would only address the multihoming across various IP links and not across multiple network technologies.

3.5.4 IP - End State [28]

The Multi-6 working group within the IETF is actively addressing the issue of multihoming for IPv6. It is anticipated that this effort will result in a robust solution that provides network layer multihoming over IP networks. The following bullets summarize the range of solutions under investigation by the IETF Multi-6 Working Group:

- IPv6 Routing Solutions. Uses the IPv6 routing system like the IPv4 approach but also adds mechanisms to alleviate the scalability problem of injecting prefixes into the Default Free Zone (DFZ).

- Identifier and Locator (Dual Space) Solutions. With a dual space solution there is a separation between the identity of a node (denoted by an identifier) and its location in the Internet (denoted by a locator).

- Mobility Solutions. One can view mobility as a special case of multihoming. When a host moves in the Internet and acquires a new address at its new location this is analogous to a re-homing event where the host's primary provider has become unreachable and must switch to using an address corresponding to one of its other providers.

- Transport Solutions. Changing an IPv6 address during the lifetime of a connection will break the semantics of that connection in common transport protocols and other Upper Layer Protocols (ULP). If the IPv6 address change is not hidden from the transport layer as with mobility or dual space solutions, then the support for address changes can be added to the transport protocols.

- Site Exit Router and Host Behaviour. Some multihoming solutions can be achieved by modifying the behaviour of a site's exit routers and/ or end hosts. This provides some multihoming support without the need for new protocol development and code installation on the site exit routers and/or end hosts.

3.6 Policy Based Routing [7]

Policy Based Routing (PBR) is the ability for packets to be routed over particular air-ground sub-networks based upon user defined rules. This is relatively straightforward for packets leaving the aircraft, but less obvious for packets destined for the aircraft. A customer may define several reasons (policies) for selecting particular routes for packets. In aviation, some of the key concerns are: link availability, link latency, message priority, service pricing and regulatory restrictions. Certain links are restricted to carrying only certain classes of traffic due to the designation of the allocated spectrum. As such, it is necessary to assure that these restrictions are abided. PBR is one way to solve this problem, however defining aircraft domains and separating these domains with VLANs might offer an alternative solution. The other key concern for airlines is service rates. Classically, VHF ACARS is much less expensive than HF ACARS which in turn is less expensive than ACARS over SatCom. This is important as the airlines would like to manage their service costs.

Like multihoming, policy based routing is a solution to a set of problems that is being incorrectly identified as a system or service requirement. Future RCP efforts need to re-assess this requirement and understand the Mission Needs that drove this design feature. In particular, it is important to understand what considerations (or policies) must be accounted for in route selection and which of these policies are requirements versus objectives.

Despite the recommendation to re-assess this requirement, a brief analysis was conducted to understand how PBR is currently handled by ACARS and ATN/CLNP and what mechanisms could be provided by IP both in the near and far term to provide such functionality if deemed necessary. Table 8 summarizes key comparative aspects of the policy based routing architectures while the following sections describe these architectural aspects in further detail.

Table 8 Policy-Based Routing Comparison

	ACARS	ATN/CLNP	IP Near Term	IP Far Term
A-G Route Selection Element	MU	CMU	Airborne message router or airborne SCTP gateway	CMU/Airborne IP Router
G-A Route Selection Element	DSP	ATN/CLNP Router	Terrestrial message router or terrestrial SCTP gateway	TBD (based upon the outcome of Multi-6 effort), possibly the Home Agent
PBR Protocol	Proprietary	IDRP (w/	Proprietary messaging based or SCTP (may	TBD (based upon the outcome of the Multi-

		customizations)	require extension)	6 effort)
Source of Policy	Downlink in MU, Uplink in DSP	Defined in ATN/CLNP Router and propagated through the network	Defined by airborne MSG router or SCTP gateway and exchanged with terrestrial counterpart	TBD (based upon the outcome of the Multi-6 effort)

3.6.1 ACARS

For downlink messages, custom functionality is employed within the MU/CMU to send messages over links in a priority order depending upon link availability. For uplink message a similar routing policy is employed by the DSP to determine the order of links attempted subject to availability.

3.6.2 ATN/CLNP

As discussed earlier, the ATN/CLNP-customized IDRP protocol includes provisions to define routing policy and to exchange this routing policy as part of its route advertisement and distribution function. Therefore, the airlines configure their airborne ATN/CLNP routers with the desired routing policy and this policy is distributed through the ATN network when the aircraft joins or moves through the network.

3.6.3 IP – Near Term

In the near term, the policy based routing functionality would either be accommodated in the airborne and ground message routers via topic based routing features or the desired logic would be configured into the SCTP gateway. In this scenario, the gateway would be designed to exchange this policy information with its terrestrial endpoint upon connection establishment.

3.6.4 IP - End State

Policy based routing is a critical component of network layer multihoming. If a router has multiple options for forwarding a packet to a particular address, some form of policy is required to select a route. As such, this functionality is also being addressed by the Multi-6 working group.

3.7 Multicast [7]

Multicast allows a packet to be sent simultaneously to a configurable and manageable group of users. This function is very useful to support classes of broadcast communication services such as push to talk (PTT) voice and broadcast data services such as TIS and FIS. Obviously PTT voice is an intrinsic capability of an analog half-duplex communication system. However, with the move toward integrated voice and data services over a single medium, multicast data distribution has become a key feature of most proposed PTT voice solutions of a packet data network.

Data broadcast services such as TIS and FIS are currently offered as Layer-2 broadcast services. This is a viable alternative but does introduce certain shortcomings. In particular, the broadcast ground station must be connected directly to an application that generates the data stream. Granted this direct connection may be remote (via a X.25 link) but the ground station cannot just be connected to a data network. The advantage of direct connection to a data network is that ground stations (such as VDL-B) could offer multiple logical channels to carry various services such as TIS-B, FIS-B, LAAS broadcasts and potentially also handle some bi-directional data messaging. Such a configuration provides for a decoupling between the datalink infrastructure and the network services they support.

Table 8 summarizes key comparative aspects of the multicast architectures while the following sections describe these architectural aspects in further detail.

Table 9 Multicast Comparison

	ACARS	ATN/CLNP	IP Near Term	IP Far Term
Addresses	Broadcast address	NA	Yes	Yes
Group Management	No	NA	Yes	Yes
Protocols	NA	NA	IGMP, BGMP, MLD, PIM-SM	IGMP, BGMP, MLD, PIM-SM

3.7.1 ACARS

ACARS provides a message broadcast capability to all aircraft and provides features to allow specific multicast groups such as multicast to all of an airlines aircraft or all aircraft of a particular model. However, ACARS does not provide robust multicast group management features that would allow for the dynamic creation and management of multicast groups as would be required to accommodate many of the service needs.

3.7.2 ATN/CLNP[12, 13, 14, 15, 16]

ATN/CLNP does not provide multicast services. An explanation provided for this omission[13] was that ATN/CLNP was intended to only support guaranteed delivery services. Since receipt acknowledgement of multicast packets is an onerous problem, the delivery of multicast services was not pursued.

3.7.3 IP – Near Term [7]

In the near term, the multicast function can be achieved using the IP multicast protocols available for IPv6. Hosts wanting to join IP-multicast groups would need to support Multicast Listener Discovery (MLD) for IPv6 as defined in RFC 2710 for communication with their mobile router. A large selection of protocols is available for communication between routers as necessary to manage the addition and deletion and of nodes to the routing tree and the routing of packets through the multicast tree. Distance Vector Multicast Routing Protocols (DVMRP – RFC1075), Multicast Open Shortest Path First (MOSPF – RFC1584), Protocol Independent Multicast – Sparse Mode (PIM-SM RFC2362) and Border Gateway Multicast Protocol (BGMP) are potential protocol components to implement IP multicast within the MCNA. However, more research is required to investigate these design alternatives and assure compliance with FTI terrestrial IP network design.

3.7.4 IP - End State

In the end state, the IP solution for multicast should be the same as for the near term.

3.7.5 Layer-2 / Layer-3 Coordination and Efficiency

IP multicast is implemented as a means of restricting unnecessary use of system capacity to distribute common information to multiple users. A roughly comparable service could be achieved using a publish/subscribe server that receives a packet, replicates it and sends copies out to all of the subscribing hosts. Since the Air-Ground sub-networks are typically the most constrained resource, it is desirable to assure an efficient mapping between the network layer and A-G sub-network.

IP multicast uses a routing tree to distribute packets. In the case of PIM-SM, requests to join a multicast group are forward up the tree to the base, called the Rendezvous Point (RP) and multicast enabled routers along this tree add routes necessary to accommodate the request. The critical design aspect in the MCNA implementation of multicast is how the aircraft are treated with respect to the access point that they are attached. A terrestrial network typically has a separate link between each pair of connected routers. In wireless networks, a group of routers may be connected over a shared link to a single access router. Ideally the multicast enabled access router will treat a shared connection by

[13] Aloke Roy, Honeywell, provided this explanation from his experience helping to develop the ATN/CLNP specifications.

multiple subscribing aircraft as such and only broadcast (or layer-2 multicast) the packet once rather than forwarding the packet individually to each aircraft. This interface can become particularly complex with satellite systems or terrestrial base stations that have multiple beams. In this case, each beam should be treated as a separate connection and multicast packets should be forwarded to each beam that has active subscriptions to the applicable multicast group.

3.7.6 Coordination with FTI

Acknowledging that MCNA will need to interface with with ground networks implemented by various FTI link service offerings, the MCNA multicast architecture will need to be compatible with IP multicast services provided by FTI if and when those services become available. This should not be a significant coordination effort given that IP multicast is fairly standard and the Layer-2/Layer-3 multicast interface for which we are concerned is implemented at the access routers which would typically be within the domain of MCNA rather than FTI. However, specific IP multicast protocols such as PIM-SM and BGMP should be coordinated. At this time our access to specifics about FTI is limited. However, given our knowledge of the transition plan for FTI, it is anticipated that IP multicast considerations will be addressed at later stage of that program.

3.8 Quality of Service

Quality of Service (QoS) is a heavily loaded term with many different meanings depending upon the specific context. For the purposes of this discussion, QoS refers to those mechanisms within the architecture that enable the network to provide services meeting the advertised performance specifications (latency, throughput, availability, continuity, etc.) and that allow a network to degrade gracefully during unanticipated loads or failure scenarios.

This discussion begins with a survey of QoS mechanisms available at the applicable layers within the OSI reference model. As well, a quick discussion is offered regarding the interaction of QoS mechanisms between Layer-2 and Layer-3 in wireless networks. With this background, an overview is provided of the mechanisms provided and planned within the various internetworking protocols (Layer-3) under consideration for MCNA.

3.8.1 Layer-1 QoS Mechanisms

Wireless links tend to be very lossy and mobile wireless links are typically dynamic. Therefore, careful consideration must be provided for mechanisms that maintain reasonable link quality (and therefore Bit Error Rate (BER)) under these conditions. Commonly used techniques include:

- Forward Error Correction (FEC) – mechanisms that allow the detection and correction of bits that are determined to be in error. Using FEC introduces an overhead that results in diminished channel throughput but increases the BER performance. Examples include: Reed-Solomon codes, Convolutions codes and Turbo codes.

- Error Detection – mechanisms focused on detection of errors without correcting these errors. These mechanisms provide much better error detection performance with significantly less overhead. They are often used together with FEC to assure much lower probability of undetected BER for services that are sensitive to undetected errors. Examples include parity bits and Cyclic Redundancy Check (CRC).

- Adaptive Waveforms – Given dynamic link conditions, some wireless protocols employ a family of waveforms that offer varying throughput and associated link margin. Link performance is continuously monitored and when link conditions deteriorate, the waveform is changed to adapt to the link condition by providing lower throughput but acceptable loss. Conversely, as link conditions improve, the waveform is changed to maximize throughput.

3.8.2 Layer-2 QoS Mechanisms

Layer-2 begins to introduce mechanisms that dynamically differentiate the service quality for various services. Wireless links tend to be asymmetric from the perspective of QoS mechanisms since they are a shared media. The point-to-multipoint nature of the interface offers more effective QoS mechanisms for traffic that is flowing from the single access point out to the multiple mobile nodes (forward link). In contrast, prioritization of traffic flowing from these multiple disparate nodes back to a single access point (return link) requires more complex mechanisms. The primary QoS mechanisms offered at Layer-2 are outlined below:

- Automatic Repeat Request (ARQ) – this family of mechanisms employs state machines at either side of the link that monitors the flow of traffic, identifies when a packet is not received and signals the complementary state machine to retransmit the lost packet(s). Multiple variations on this technique exist and vary in complexity, effectiveness and overhead. Use of this function results in what is known as a Reliable Link Service (RLS).

- Priority queuing – Layer-2 packets are marked with a discrete priority and entered into a queue representing that priority. The link service delivers packets in strict priority queue order delivering packets by queue priority in a First In First Out (FIFO) order. This technique is very effective on the forward link where all traffic to a group of users sharing a channel arrives at an access point for queuing and delivery, thus assuring prioritization of packet delivery between users. However, this technique is less effective on the return link. Each mobile user can apply priority queuing to assure that the aggregate of traffic they send to the access point is transmitted in the proper order but the mobile users do not have knowledge of the queue state of other users sharing the channel. Obviously, the effectiveness of this technique is fully dependant upon the Media Access Control (MAC) technique applied.

- Demand Assigned Multiple Access (DAMA) – DAMA is a class of MAC that requires all of the users sharing a channel to make periodic requests for return link resources based upon the status of their queues. The DAMA processor, located at the access point, aggregates the resource requests and allocated resources in priority order. This MAC technique, extended to provide QoS support, addresses the QoS shortcomings of priority queuing on the return link.

3.8.3 Layer-3 QoS Mechanisms

The Layer-1 and Layer-2 QoS mechanisms described above are important to assure QoS is maintained over the wireless links. However, those mechanisms only apply to a single link and do not assure end-to-end QoS. The internetworking layer (Layer-3) is the lowest level of the protocol stack that extends end-to-end and is therefore a key factor in assuring service quality. As such, a wide assortment of QoS mechanisms has been developed at this layer, a few of which will be described below in further detail.

- Priority queuing – very similar to the equivalent mechanisms at Layer-2, priority queuing applies a priority to each packet traversing the networking and all of the routers use this priority to queue packets and service their queues in the same manner as described for Layer-2. Priority queuing is a statistical QoS mechanisms because no guarantee is provided that packets will be delivered within a specified time. QoS policy is defined on a Per Hop Basis (PHB) and through the application of the same QoS policy across the entire network, statistical service quality guarantees can be offered.

- Differentiated Services (DiffServ) – DiffServ is an extension of the priority queuing concept to include additional mechanisms besides strict priority scheduling and queue management techniques at the routers. Additional techniques such as Round Robin, Weighted Round Robin, Weighted Fair Queuing, Random Early Discard, etc. provide the ability to tune a network to more effectively carry a mix of traffic services.

- Integrated Services (IntServ) – IntServ provides end-to-end service delivery guarantees by signaling and negotiating QoS along each link of the end-to-end path before initiating communications. This approach provides QoS guarantees but requires signaling time before initiating communications and requires compliance by all routers and links between the two end points. This later restriction has limited the use of IntServ in the public internet because it is difficult to transition a network when no benefits can be achieved until the entire network has upgraded. For the ATM environment, the network is controlled by a single entity, thus IntServ may be easier to deploy and manage[14].

3.8.4 Layer-4 QoS Mechanisms

The transport layer often provides end-to-end reliable transport (equivalent to the ARQ at layer-2) and end-to-end error detection. Common examples of this or the Transmission Control Protocol (TCP) common in the public internet that provides a 16-bit CRC for error detection and the selective repeat ARQ.

3.8.5 Layer-2 / Layer-3 QoS Interactions

One particular area of focus for wireless networks is the interaction of QoS mechanisms between Layer-2 and Layer-3. If packets are prioritized at both layers, the interactions between these two mechanisms can cause unintended results. For example, assume that a mobile router employs DiffServ and is connected to a wireless modem that employs strict priority queuing and priority-based DAMA.

Assuming the mobile link has a peak throughput of a few hundred kilobits per second but the router is connected to the modem via 100baseT Ethernet, very little egress buffering of packets would typically occur in the router. Instead, all of the egress traffic will be forwarded directly to the modem with the result that only strict priority queuing effectively occurs. This issue can be partially addressed by limiting flow between the router and the modem.

Flow limiting allows more traffic to be buffered in the router and offers the ability to apply the wider range of queue scheduling and management algorithms afforded by DiffServ. However, if the rate limiting is too severe, a modem running a DAMA algorithm is not able to maintain sufficient traffic in its queue to properly signal the access point with representative requests for resource allocations. It quickly becomes evident that the interaction of QoS mechanisms in this scenarios can be very complex and must be carefully modeled using a high fidelity discrete event simulator (DES), such as OpNet, to properly tune the configurations of the network devices. It would also be interesting to investigate the potential of a special protocol or SNDCF between the router and the modem that would allow the modem to share information about queue state that could be used by the modem to request DAMA resources.

Table 10 summarizes key comparative aspects of QoS while the following sections describe these QoS characteristics in further detail.

---

[14] The network would be made up of components from FAA, ARINC / SITA, airlines, phone companies, etc. that would require contracts and Service Level Agreements (SLA) to ensure that this IntServ is properly and consistently deployed.

Table 10 QoS Comparison

	ACARS	ATN/CLNP	IP Near Term	IP Far Term
Layer-3 QoS Mechanisms	NA	16-Level strict priority queuing	DiffServ	DiffServ
Layer-4 QoS Mechanisms	NA	TP4: 32-bit CRC and ARQ	TCP: 16-bit CRC and ARQ SCTP: 32-bit CRC and ARQ	TCP: 16-bit CRC and ARQ

3.8.6 ACARS QoS

ACARS does not provide any Layer-3 QoS mechanisms. VDL does not provide effective Layer-2 QoS capabilities but the Aero-H bearer provides a DAMA-like system with effective prioritization mechanisms.

3.8.7 ATN/CLNP QoS

CLNP provides strict priority queuing with 16 levels of priority. However, AVLC is based upon CSMA and does not provide effective QoS mechanisms on the return link. This deficiency may be remedied with the deployment of VDLm3 other future candidate link. ATN/CLNP also employs the TP4 transport protocol which offers a 32-bit CRC and ARQ mechanisms.

3.8.8 IP – Near Term QoS

In the near term, DiffServ is proposed as the primary Layer-3 mechanism for QoS. This requires compatible QoS mechanisms at Layer-2 which will not be provided by AVLC but are likely to be provided via Swift-Broadband, P34 and/or 802.X if and when they become available in the aviation environment. At the transport layer, the near term IP solution will employ either TCP or SCTP depending upon the final solution for multihoming and policy based routing. In both cases, ARQ with CRC is provided. However, the TCP CRC is only 16-bit which has been brought into question by the ATN community[15]. SCTP does provide a 32-bit CRC which is equivalent to TP4.

[15] TCP has a standardized option for alternate CRCs in RFC 1146. Additionally, RFC 2385 notes the TCP option for a MD-5 hash algorithm for digitally signing messages which would also provide better error detection.

3.8.9 IP - End State QoS

In the end state, DiffServ is still the proposed Layer-3 QoS mechanism. However, IntServ should be reviewed at a later date to determine if services with tight latency restrictions such as voice will require a more deterministic QoS mechanism to assure service quality. At the transport layer, TCP is more desirable because it is more commonly used in the internet and will be supported by COTS products. However, further analysis is required to determine if the 16-bit CRC provided be TCP is a significant deficiency requiring the selection of an alternate transport protocol or extension to TCP.

3.8.10 Coordination with FTI

The QoS architecture, particularly for both the near term and far term IP solutions must be compatible with FTI. Given the limited availability of detailed technical information on FTI, this will need to be the subject of future research activities.

3.8.11 Coordination with SWIM

SWIM is concerned with QoS both from the perspective of data transport and message handling. As such, SWIM will rely upon QoS mechanisms provided by FTI and MCNA but also introduce QoS mechanisms at higher layers to assure that information request are addressed in the appropriate order. In the case of the near term IP architecture, additional overlap may exist between the MCNA and SWIM QoS architectures. In particular, the SWIM message routing function employed by MCNA will likely introduce message header fields and associated message queue servicing algorithms. MCNA will need to conduct research to determine if these application layer QoS facilities should be employed and if they are what QoS interaction consideration must be addressed.

3.9 Security

Aeronautical communications have historically been conducted through small, application specific, closed networks. Recently, the desire has arisen to provide network connectivity to the aircraft in support of wide ranging applications from aircraft control to passenger entertainment and productivity. One of the major thrusts of MCNA is to provide common networking infrastructure that can handle all of these needs and thereby improve the investment analysis justification for airlines to equip. While such network integration improves the cost benefit equation, it introduces a family of security issues that must be carefully addressed. These newly introduced security needs are coupled with basic security needs that have not historically been considered for aeronautical communications and have just recently started to be addressed.

Due to the complex nature of the security problems, this discussion on security is divided into three focus areas: application security, network security and aircraft LAN security (Table 11). Application security represents end-to-end security associations between pairs of communicating applications. Application security is very effective but does require hosts to create a separate security association for each active application that requires secure communications. Network security represents all security mechanisms below the application layer including link layer, network layer and transport layer security mechanisms. These security mechanisms create secure associations between hosts, routers or modems which can then be used commonly by all supported applications. Aircraft LAN security represent mechanisms such as logical and physical sub-network separation, firewalls, etc. which provide protection of the various aircraft LAN network domains.

The following sections describe the security mechanisms employed by or proposed for the various networking technologies under consideration.

Table 11 Security Comparison

	ACARS	ATN (CLNP)	IP Near Term	IP Long Term
Application Security	NA, possible with Secure ACARS based upon ATN Security Services	ATN Security Services	Limited SWIM Security Services (based upon ATN security services)	Limited SWIM Security Services (based upon ATN security services)
Network Security	NA	NA Selective Link Authentication / Encryption	IPSec (maybe, between message routers) Selective Link Authentication / Encryption	IPSec (defense in depth has costs that must be traded) Selective Link Authentication / Encryption
Aircraft LAN Security	NA, restricted physical access	NA, restricted physical access or AFDX	AFDX for aircraft control domain, Firewalls, etc.	AFDX for aircraft control domain, Firewalls, etc.

3.9.1 ACARS

Application Security: Currently ACARS does not provides application security. However, Honeywell has developed a concept, called Secure ACARS, which provides application security using similar mechanisms as defined within the ATN security framework.

Network Security: ACARS does not provide Layer-3 security. Some of the A-G sub-networks employed by ATN may provide link layer security.

Aircraft LAN Security: Restricted physical access via closed networks.

3.9.2 ATN/CLNP [12, 13, 14, 15, 16]

Application Security: Security has been a key focus of the ATN development and has resulted in an application security framework that appears very comprehensive and is consequently being recommended for reuse widely within the industry.

Network Security: CLNP does not provide Layer-3 security. Some of the A-G sub-networks employed by ATN may provide link layer security and IP-based G-G ATN transport may provide IPSec security.

Aircraft LAN Security: Restricted physical access via closed networks.

3.9.3 IP – Near Term [11]

Application Security: SWIM is working on developing and providing as a service an application security suite that is very similar to the ATN security framework. The near term IP solution would employ the SWIM security services.

Network Security: In the near term, IPSec might be used between the airborne message router and the terrestrial message routers. However, such added security must be traded against the resultant latency in setting up connections to determine the optimum balance. Similar to ATN, certain A-G sub-networks may provide link layer security mechanisms that would further protect A-G communications.

Aircraft LAN Security: Given the intent to migrate all classes of aeronautical communications to IP, special care must be taken to separate the aircraft LAN into domains and protect each of these domains from potential threats in the other domains. Figure 17 depicts a notional aircraft LAN security architecture. Each sub-network domain is physically separated and protected behind a firewall. The aircraft control domain uses AFDX, further limiting the ability for intrusion by a non-configured user. A VLAN is used between the aircraft domains and the modem to provide each domain access only to those A-G links that can support the associated class of traffic.

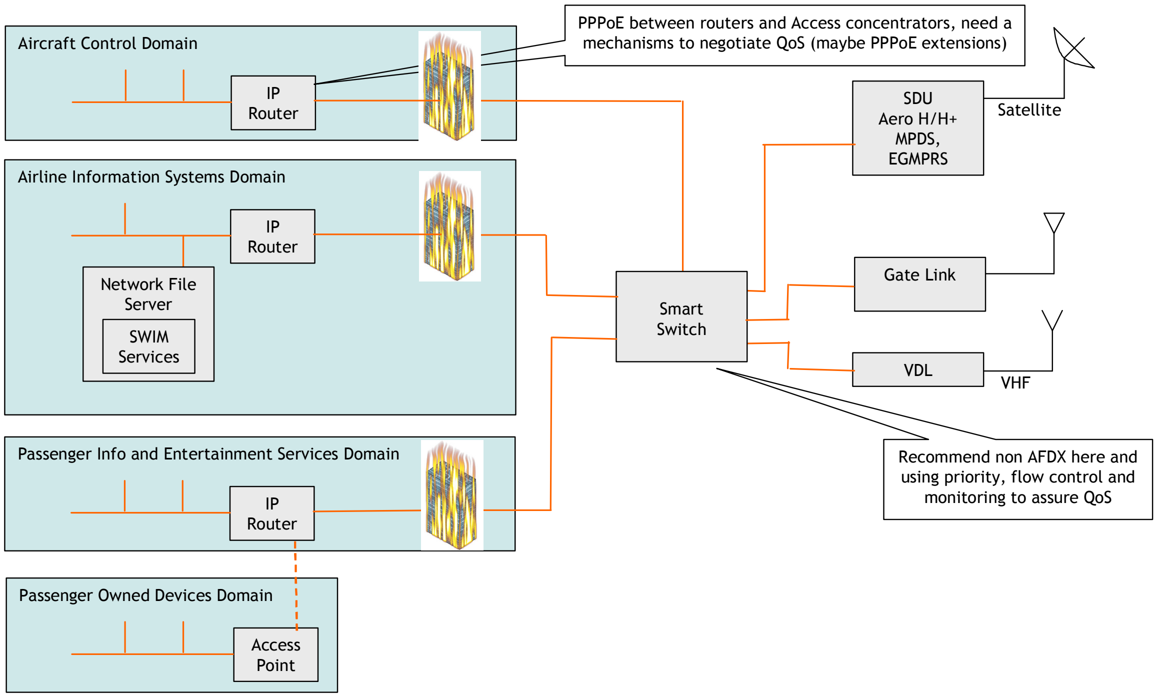

Figure 17 IP-based Aircraft LAN Security Architecture

3.9.4 IP - End State [7]

Application Security: Based upon the SWIM security service, as with the IP near term security architecture.

Network Security: In the far term, network layer security via IPSec or equivalent will become an integral aspect of the network security architecture. Similar to ATN, certain A-G sub-networks may provide link layer security mechanisms that would further protect A-G communications.

Aircraft LAN Security: Same as the IP near term.

3.9.5 Datalink Sub-Network Unique Security Considerations

One of the security concerns for Air-Ground communications that has received significant attention is the threat of RF jamming. RF jamming is really a subclass of network security threats termed Denial of Service (DoS) and in some ways is one of the least threatening because the attack is restricted to the physical layer and only denies access to spectrum. More complex DoS attacks masquerade as real users attempting to use the system, flooding the connection with system control messages that take away bandwidth and utilize all available processing capability while the modem, router, host, etc. attempts to process these control messages. Such an attack could render all A-G links ineffective if the attacker is successful in completely utilizing resources that are shared across all of the A-G links.

Without applying military Anti-Jamming (A/J) technology, the resistance of a link to an RF jamming based DoS attack is only effective if the attack is relatively unsophisticated. A more effective solution to RF jamming based DoS is to provide a multi-spectral, multi-homed connection to the aircraft. It would require an extremely sophisticated attack to deny both a terrestrial VHF and L-band SatCom link simultaneously. In summary, MCNA provides RF jamming attack resistance by supporting multiple different A-G links.

Another datalink sub-network security consideration is the passing of security credentials during link handoff. Since link handoffs can be rather frequent and the time to establish link layer security credentials can be significant relative to the latency requirements of some communication services, re-establishing these credentials with each link handover may prove unacceptable. If the datalink sub-network offers provisions to assure a make-before-break handoff, this concern is diminished because dual links can persist until the new link is fully functional. However, without such provision, it is typically desirable for the datalink sub-network to accommodate the transfer of link level security associations during link handoff.

3.9.6 Coordination with SWIM

The application security for SWIM-enabled applications is based upon SWIM security services and therefore should be fully compatible. Generally, network security mechanisms are independent of SWIM and should therefore not require coordination. They should however be coordinated with CDT as discussed in the following section. The transport layer represents some degree of overlap in scope of responsibility between SWIM and MCNA/CDT. However, from the perspective of security, no mechanisms were defined at the transport layer. Therefore, the security mechanisms defined by SWIM should be accommodated without conflict.

3.9.7 Coordination with FTI

Network security mechanisms for MCNA should be consistent with the FTI security architecture. At this time, our limited exposure to FTI architectural information prevents us from commenting on the degree to which this is currently coordinated. A recommended action for future MCNA development would be assuring such coordination.

In order to support FAA safety services, the FAA requires the development of several security documents. One of these documents is the Protection Profile (PP). An MCNA Protection Profile would be based upon the High Risk NAS WAN PP Template. This should be the same as the FTI PP. The FAA has already created templates for these documents. Therefore, the effort required to develop an MCNA PP would simply entail minor modification of the appropriate template (mentioned above) with descriptive information about MCNA. A link to the appropriate PP template is provided below.

http://www.faa.gov/aio/ChiefSci/pp_library/documents/HRNASWAN1-0.pdf

3.10 Network Management

3.10.1 FCAPS

The MCNA should encompass network management functionality (as was described in the functional analysis) including functions for Fault Management, Configuration Management, Accounting, Performance Management and Security Management. While Network Management encompasses a large portion of the functionality, it is somewhat generic functionality that should be addressed more thoroughly during later program development stages.

3.10.2 Coordination with SWIM

The MCNA Network Management functionality should be coordinated and consistent with the SWIM systems management capabilities as described in the SWIM architecture Document (D794-10166-1) [11].

3.10.3 Coordination with FTI

As an extension of the CDT, the MCNA Network Management should be fully compatible with FTI. FTI Network Management Operations includes a Network Operations and Control Center (NOCC) in Melbourne, FL and a backup NOCC in Chantilly, VA. The FTI Network Management and Operations (NMO) function provides the following capabilities:

- Monitor and measure performance
- Generate alarms and alerts
- Manage trouble tickets
- Provide real-time status
- Provide daily performance summary
- Provide service reference information
- Provide access to selected CDRL's
- Archive critical data and provide online access for 12 months
- Manage preventative and corrective maintenance
- Provide customer care/support

Since MCNA services will integrate with FTI services to create end-to-end communications services, it would be advisable to integrate the network management functions. Given that the FTI NOCCs and NMO functionality are already established, it would make sense to leverage and augment this capability as applicable to meet the unique needs of MCNA.

3.11 Network Protocol Accommodation

The discussion thus far has focused upon the network architecture considerations for each network protocol. In most cases, an application on the aircraft will be associated with a single network protocol while the available air-ground links relate to multiple network protocols. Consequently, this section considers accommodation between network protocols.

Initially, an exercise was conducted to consider avionics configuration variants that included multiple network protocols. This exercise assumed that each aircraft's flight management computer (FMC) would support only one network protocol. While subsequent research has determined that this is not in fact a steadfast rule, it proved a useful assumption for this exercise. Given this assumption, Table 12 was developed to provide reasonable examples of aircraft configurations. Terminology from the Boeing Datalink Strategy was employed to describe FMC configurations. FANS 1/A represent a datalink enabled FMC using ACARS, FANS 2 with ATN/CLNP and FANS 3 with IP. For aircraft configured as FANS 1, 2 or 3, multiple variants were defined based upon combinations of air-ground datalink avionics that seemed reasonable. This exercise verified the hypothesis that aircraft would likely be equipped with a mix of datalink network protocols and would thereby benefit from the ability to provide accommodation between network protocols to enable enhanced communication service classes and levels.

Given confirmation that protocol accommodation is a useful service, a table was developed to investigate what viable means of protocol accommodation are available for pairs of network protocols (Table 13). Three primary means of protocol accommodation were considered: message tunneling, network tunneling and parallel networks. Parallel network means that a given candidate link is either capable of or modified to support additional network protocols. An example of this would be AVLC (VDLm2) which supports CLNP, ACARS and may soon support the transport of IP packets. Technically, parallel networks are ideal. However, the cost to deploy ACARS, ATN/CLNP and IP networks to all of the VHF ground stations (for example) may prove cost restrictive. Network tunneling treats a connection through one network as a logical datalink connection for another network. This approach can reduce cost, but results in the application of redundant headers and the associated overhead and latency. The third accommodation mechanism under consideration is application messaging. This is a favorable alternative given the previously stated intention to use message routing as a means to integrate with SWIM and resolve the mobility, multihoming and PBR requirements for near term IP. Since most of the communication application are message-based, a message routed infrastructure could be employed that is network protocol independent.

Table 12 Examples of Aircraft Configurations Supporting Multiple Network Protocols

Aircraft Avionics Options	Technology Pair	Description	Example
FANS 1/A (ACARS)	ACARS	One of several thousand FANS or POA/AOA aircraft today	Aero-H
	ACARS + IP	FANS aircraft with Swfit64/BB cards in the SatCom unit	Aero-H + Swift64/BB
FANS 2 (ATN)	ATN	Link 2000+ aircraft	ATN/VDLm2
	ATN + ACARS	Link 2000+ with POA/AOA	ATN/VDLm2 + POA/AOA
	ATN + IP	Link 2000+ with Swift64/BB or CbB	ATN/VDLm2 + Swift64/BB
	ATN + ACARS + IP	Link 2000+ with Swift64/BB or CbB and POA/AOA	ATN/VDLm2 + POA/AOA + Swift64/BB
FANS 3 (IP)	IP	Swift64/BB and/or P25/34	SwiftBB/P25/P34
	IP + ACARS	Swift64/BB and/or P25/34 and POA/AOA	SwiftBB/P25/P34 + POA/AOA

The protocol accommodation table was developed by considering the viability of each of the proposed techniques to provide protocol accommodation between pairs of network protocols. The table is laid out to investigate how each of the network protocols could accommodate each of the other network protocols. The diagonal was blacked out since it signifies a protocols ability to support itself. ACARS, as the original and most primitive network protocol is not deemed capable of accommodating CLNP but is believed to be able to accommodate IP-messaging by encapsulating the messages into ACARS plain-text messages to create a message bridge. ATN/CLNP is capable of accommodating ACARS via network tunneling[16] or message tunneling. Likewise, ATN/CLNP could accommodate IP using either of the same means.

[16] GACS provides this service however this solution has not been commercially adopted and other more viable alternative exist.

Table 13 Accommodation between Network Protocols

Protocol making Accommodation

Protocol being Accommodated	ACARS	ATN (CLNP)	IP
ACARS		Messaging or Network Tunnel	Messaging or Network Tunnel
ATN (CLNP)	NA		Network Tunnel (with SNDCF to move mobility and multi-homing responsibility entirely to ATN)
IP	Messaging	Messaging or Network Tunnel	

IP could accommodate ACARS via messaging or a network tunnel. The messaging solution could either integrate with the ACARS datalink service provider network or bypass them completely using the SWIM message routing service. However, network tunneling would entail an IPSec tunnel from an airborne host or router down to an IP/ACARS gateway and is therefore dependant upon support from the datalink service provider. IP support of ATN/CLNP is limited in the near term due to insufficient support of mobility, multihoming and policy-based routing capabilities. However, a custom SNDCF for CLNP over IP could be developed that treats IP connections as transient datalink connections above which CLNP manages all of the mobility, multihoming and PBR functions.

4 MCNA AVIONICS ARCHITECTURE

4.1 Introduction

While the network-centric SWIM environment is intended to transform operation of the NAS, operational and air traffic efficiency are further enhanced when IP-based SWIM services are available to each aircraft. Recently, commercial networks supporting Internet Protocols are increasingly being installed on aircraft for both on and off-board communications although operational and air-traffic services are still using dedicated, legacy air/ground networks (e.g., VDL, ACARS). Therefore, it is essential to modernize the avionics architecture to seamlessly and cost-effectively extend the SWIM services to aircraft by leveraging the IP-based commercial networks while assuring the safety of flight.

As part of the overall MCNA Architecture effort, the avionics architecture task focused on definition of a vision-state architecture that incorporates functionality necessary to support present, near-term and envisioned operations/scenarios. The avionics architecture task included:

- An assessment of the current state of existing fielded avionics architectures and current trends toward network-centric and IP-based avionics,
- Definition of a proposed vision-state architecture, including identification of technology gaps, risks, and potential mitigation strategies,
- Identification of transition concepts, particularly operation with mixed avionics architectures, and
- Identification of standardization actions necessary to support the vision-state architecture.

The avionics architecture discussions presented in Section **Error! Reference source not found.** focuses on complex aircraft installations where advanced, computerized systems are used for flight and operational control, in-flight entertainment and passenger services. Network-centric SWIM services are more relevant to transport-class, high-end BA and GA aircrafts. It is unlikely that digital avionics with integrated information management and data communication capabilities will extend to the low-end GA aircraft in the foreseeable future. The satellite-based, handheld moving-map displays, weather graphic overlays, and personal computers with WiFi communication systems are not integrated in the low-end GA aircrafts. These systems are considered to be Passenger Electronic Devices (PEDs) and are not explicitly covered by this study.

4.2 Avionics Starting Points

This section describes the current, “as-is” avionics architecture related to MCNA. There are two predominant, current architectures: federated, comprised of individual hardware devices; and integrated, consisting of large hardware platforms running multiple software applications on different hardware subsystems. This section also addresses avionic architectures that have been proposed recently in various forums, such as the architecture demonstrated in GCNSS Phase 1 and defined in the ARINC Specification 664, "Aircraft Data Network (ADN)".

4.2.1 Federated Avionics Architecture

Traditionally, aircraft communication systems have been implemented using federated avionics architectures. As user needs evolved over the last three decades, various communication capabilities were implemented by dedicated hardware devices or Line Replaceable Units (LRUs) to satisfy those needs. Figure 18 illustrates the current aircraft audio communication architecture, where multiple audio management units communicate with a federated group of communication radios and a federated group of navigation receivers through dedicated, primarily analog, interfaces.

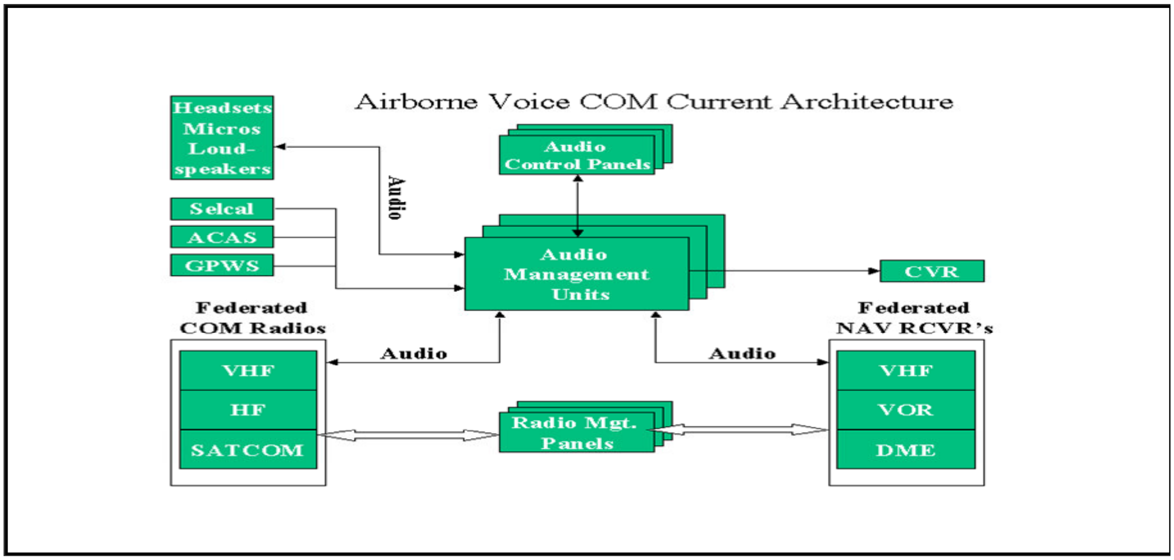

Figure 18 Current Federated Audio Communications Architecture

As shown in Figure 19, the federated aircraft data communication architecture employs the Communication Management Functions (CMFs) to communicate with federated data radios such as HF, VHF, SATCOM, Mode-S, UAT, etc. Usually, the transoceanic aircraft have capability to communicate over HF or SATCOM media. VHF is the predominant mode of line-of-sight data communications. In older aircraft configurations where only two VHF radios exist, one VHF radio is shared for both voice and data communications. The crew selects the communication mode through the audio management system. In newer, three-radio configurations, a VHF radio is dedicated for data communications but can be switched to voice mode if one of the voice radios fails. The first generation of VHF data radios only support analog interfaces while all HF, SATCOM and newer VHF digital radios (VDRs), comply with ARINC 429 digital interface standard.

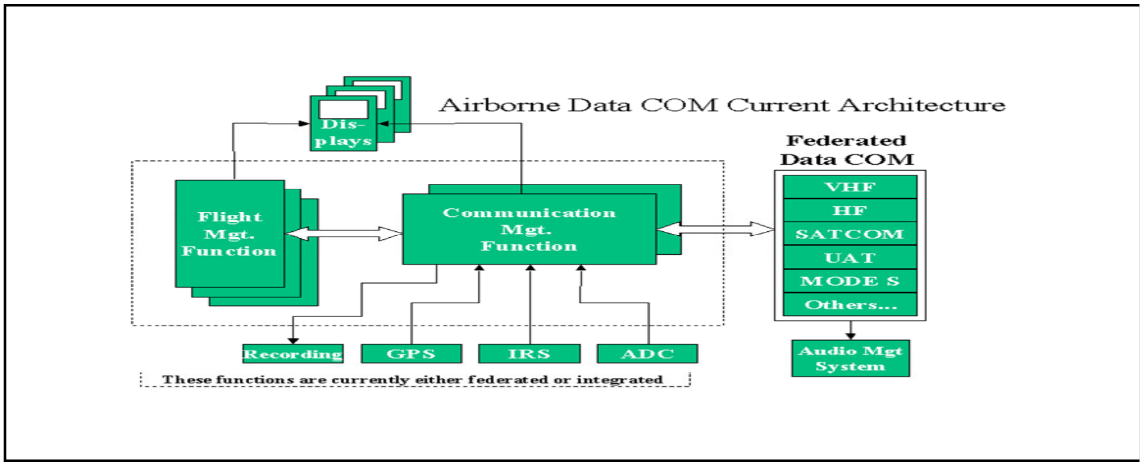

Figure 19 Current Federated Data Communication Architecture

As each LRU performs a specific functionality, it is designed to provide optimum performance at lowest possible cost, which is the biggest benefit of the federated architecture. The dedicated functionality also simplifies the LRU certification process. However, the design optimization makes the LRUs incompatible with each other, and functionally non-interchangeable, which drives up the cost of operation, implementation, maintenance, and logistics.

4.2.2 Integrated Avionics Architecture

With technological advancements, the avionics industry is driving towards more integration among subsystems as illustrated in Figure 20. In later generation aircraft such as the Boeing 777, Airbus 340, Airbus 380 and business/regional jets, the CMF has been integrated with the Flight Management Function. Similar integration has been carried out in the high-end General Aviation (GA) avionics. This trend relies on software defined functions over a limited number of common hardware platforms. Using groups of common components, each platform is programmed differently via software. Multiple platforms, configured to perform one or more functions, are located in a single LRU, i.e. several hardware cards in slots on a common shared bus. The single data bus supports different traffic types, such as critical air traffic and essential operational services. Therefore, this bus needs to have deterministic behavior with guaranteed delay/throughput performance. Such determinism is usually implemented through Priority, Precedence, and Preemption (P3) mechanisms.

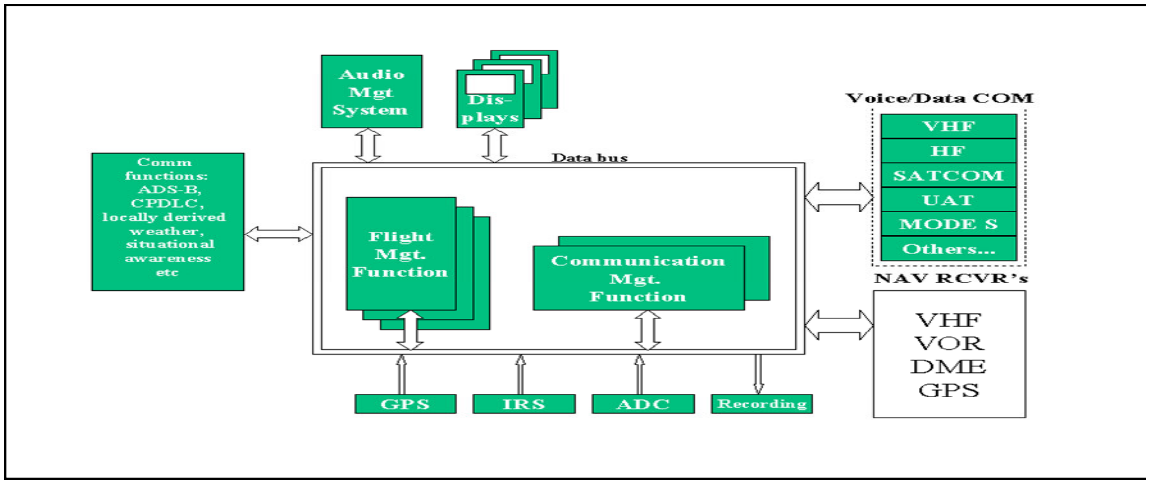

Figure 20 Integrated Avionics Architecture

Digital signal processing (DSP) hardware permits further integration of communication and navigation transceivers through software defined radios (SDRs). The SDRs use the same software components but exercise different configuration parameters to provide different communication, navigation, and surveillance (CNS) capability. This software-defined radio concept is implemented in ARINC 750 compliant VDRs. The SDR trend will continue in the future where a single LRU will be dynamically reconfigured to perform one or more CNS radio functions as shown in Figure 20.

Since the SDR utilizes common hardware and software-defined components, it lowers development, integration, logistics, operational and maintenance cost. It enhances resource allocation and information sharing among airborne subsystems. Overall system availability may be improved at a lower cost by leveraging *n-of-m* redundancy of system components. By appropriate design of the common hardware and software elements, the integrated SDR architecture may acquire certification credit due to reuse. One major concern of reuse is that it may introduce a single point of failure, where a common hardware component failure or software component error affects multiple functions. Current safety-critical architectures often use "dual-dissimilar" designs, where the critical function is implemented in independent hardware using different implementation designs. In SDR architecture, safety-critical functions that require very high integrity might still drive towards dissimilar implementations to reduce the probability of multiple subsystem failures arising from a common cause.

4.2.3 GCNSS-I Demonstration Architecture

Boeing and the FAA conducted the Global Communication, Navigation, and Surveillance System Phase I (GCNSS-I) trials in 2003. The objectives of the GCNSS-I tests were to evaluate the feasibility of extending the SWIM environment to the aircraft. A Connexion by Boeing (CbB) satellite link provided IP connectivity from the aircraft to the terrestrial Common Information Network (CIN). Two-way controller-pilot voice and data communications; automatic dependent surveillance via satellite; and an uninterrupted transition between radar and offshore/oceanic air traffic domains demonstrated the global, integrated CNS and CIN concepts. The GCNSS-I demonstration showed a potential future implementation of a network centric air traffic management (ATM) and SWIM using Internet Protocol (IP) as the common transport protocol.

Use of the widely adopted IP network protocol is an essential element of the SWIM/CIN concept to achieve interoperability, scalability, cost-effectiveness, and manageability. The GCNSS team concluded that IP version 4 (IPv4) will not meet the mobility, Quality of Service (QoS), addressing, security, and multilink data delivery requirements of ATM. The IP version 6 (IPv6) standards resolve some of these limitations, such as addressing and security, but additional work is required to mitigate mobility, multilink and other shortfalls. Although the Internet Engineering Task Force (IETF) is developing standards on those aspects, the resulting standards may not be adequate for MCNA without input from the aeronautical industry.

The ICAO Aeronautical Telecommunications Network (ATN) standards were developed to provide global interoperability and mobility management across national and organizational boundaries to offer seamless air traffic services. Therefore, it would be desirable to incorporate some elements of the ATN standards into IP. However, the publish/subscribe nature of the proposed SWIM architecture is more suitable for non-real-time, strategic information exchanges whereas the ATN was designed for real-time, tactical air traffic control. Therefore, integration of ATN mobility management and multilink capability within IP to meet MCNA requirements will be a complex and costly process. A thorough cost/benefit analysis should be performed to trade-off the use of ATN for MCNA versus development/update of IETF standards.

4.2.4 Network Centric Avionics

ARINC Aircraft Data Network (ADN) Specification 664 applies commercial IETF standards to aircraft and air/ground data networking to achieve network centric airline operations. The ADN uses a domain model to differentiate aircraft functions according to their criticality to ensure flight and passenger safety. This approach permits adaptation of the IETF standards according to the criticality of the functions while limiting the number of alternatives to maximize interoperability and reduce implementation costs.

The domain model consists of four domains as shown in Figure 21. The Aircraft Control Domain (ACD) has highest level of criticality and contains the Flight and Embedded Control Sub-domain and the Cabin Core Sub-domain that support safety-critical services. The Airline Information Services Domain (AISD) contains the administrative, flight support and maintenance support functions for the flight deck and the cabin. This domain handles less critical information than ACD. At the lowest level are the Passenger Information and Entertainment Services Domain (PIESD) and the Passenger Owned Devices Domain (PODD) that support passenger entertainment and productivity.

The intent of the ADN specification is to maximize the use of commercial IP standards for network centric aircraft operations. It provides guidelines to adapt the IETF standards to meet safety, security, quality of service (QoS), network management, interoperability and mobility aspects unique to each domain. ARINC 664 defines a compliant network as one that maximally complies with the applicable commercial IP standard. A profiled network is one that deviates from these standards according to the ARINC 664 specifications. An aircraft data network may deviate from the IETF standards when the standards conflict with the aeronautical, user or regulatory environment of commercial aircraft. It may also deviate from the IETF standards when it is necessary to restrict options available in those standards to ensure safety of flight. Part 7 of ARINC Specification 664 defines Avionics Full Duplex Switched Ethernet (AFDX) as the profiled network for the ACD to achieve deterministic network performance. AFDX has been implemented in AIRBUS 380 and under consideration for Boeing 787 platform. Non-ACD domains may use standard IETF protocol suite provided appropriate security measures have been implemented by each domain to protect itself from domains of lower criticality when connectivity is required between domains, within domains and with ground-based networks.

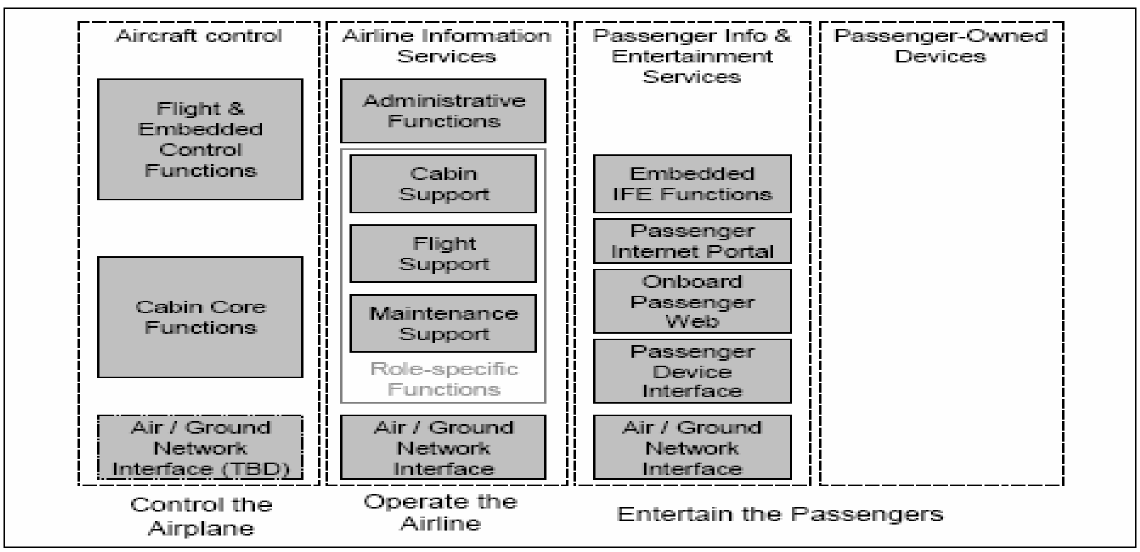

Figure 21 ADN Domain Architecture

To communicate with ground-based domains, ARINC 664 cites various communications links that are currently available or planned. The communications links include HF, VHF, satellite, wireless LAN, cellular telephone and ground-based broadband. In general, Air Traffic Services (ATS) residing within ACD are required to access only ICAO approved data links, which are Mode-S, VHF Data Link (VDL) Mode 2, Mode 3 and Mode 4, HFDL, and INMARSAT SATCOM. The VHF links can be used only for flight-safety and operational control, therefore, are limited for use by the ACD due to regulatory spectrum restrictions. SATCOM, as specified in ARINC 741/761, provides flight-safety communications[17] for the ACD. It also has a priority, precedence and pre-emption (P3) mechanism to allow non-safety communications for other domains. Non-safety communications are allowed at a lower priority than the safety communications.

All other non-ICAO specified data links, such as Connexion™ by Boeing, INMARSAT Swift 64 (S64), Iridium™ and Swift Broadband (SBB), Satellite Digital Audio Radio Service (SDARS), and Gatelink, provide non-safety communications at high data rates. These data links are targeted for use by domains other than ACD. It is possible that some applications within ACD might also use these data links provided that the QoS requirements are satisfied and adequate measures have been taken to prevent unauthorized or corrupted data to enter the ACD. ARINC 664 provides guidance on several protection mechanisms, such as firewalls and cryptographic techniques, to provide the desired authentication, integrity and confidentiality services.

4.3 Vision State Avionics Architecture

This section proposes an architecture suitable and necessary for the on-board avionics systems to satisfy the SWIM and MCNA objectives in the year 2020+. The proposed architecture has been developed with the appreciation of standardization and regulatory activities within the aviation industry and the top level MCNA requirements specified in the MCNA Requirements Report.

4.3.1 Architectural Requirements

Vision state avionics architecture will be SWIM-enabled, with the aircraft being an extension of the CDT supporting network-centric ATM. In addition, the aircraft architecture must support both tactical and strategic air traffic management to comply with the ICAO Future Air Navigation Systems (FANS) concept. This architecture should be secure, robust, scalable, adaptable, and maintainable. Maintaining a balance between all these requirements and the overarching requirements of cost-effectiveness and efficiency is the primary objective of the proposed architecture.

4.3.2 Proposed Vision-state Architecture

The domain model of the aircraft and the profiled IP adaptation approach of ARINC Specification 664 is a good framework for the vision state avionics architecture. The proposed architecture, shown in Figure 22, consists of three ADN domains: aircraft control domain, airline information services domain, and passenger and IFE services domain.

[17] Flight-safety communications, including ATS and AOC messages and services, are defined and discussed in CDRL A047, MCNA Certification Report.

As discussed in section 3.1.4, ACD contains all safety related functions that are interconnected using ARINC-664-profiled, deterministic, IP-based, AFDX network. Two essential elements of the ACD are the Network File Server (NFS), and the CMF/router functions. The NFS will be the centralized repository of information generated and/or consumed by the ACD. A few examples of these are: navigational databases, weather maps, flight manifests, electronic manuals, maintenance events/alerts/reports, etc. The NFS will provide a variety of services to support cabin-core, flight crew, flight operations, maintenance, monitoring and recording, and general aircraft administration. These NFS support services improve maintainability and robustness of the whole avionics system. The NFS performs the SWIM server and Native Application (NA) functions for the ACD. It is anticipated that the majority of installed avionics will not be SWIM compliant even by the year 2020. Therefore, the NFS will act as a SWIM Adapter (AD) for those non-compliant avionics or Legacy Applications (LA).

The CMF/router manages the network connectivity between the ACD and other on-board or off-board networks. It is anticipated that most of the air traffic services will be required to use existing, ICAO-compliant, air/ground networks such as SATCOM, VDL and HFDL. These legacy data link systems will connect to the CMF/router using the ARINC 429 Williamsburg protocol. Connectivity to other broadband networks, such as Swift64, SwiftBroadband, SDARS, Gatelink, etc. will be through a firewall and an Ethernet switch to protect the ACD from unauthorized access. Additional details on the NFS and the CMF/router is provided in Section 4.3.2.4.

The Airline Information Services Domain (AISD) provides operational and airline administrative information for the flight deck and cabin. The AISD domain handles less critical information than ACD. It consists of an industry-standard, Cabin IP LAN that connects the cabin support, flight support, maintenance support and CDS functions. The Cabin IP LAN is administered by a SWIM-based Cabin File Server (CFS). Similar to NFS, the CFS also performs SWIM server, NA and AD functions. Having two different SWIM servers in ACD and AISD domains is justified by the different criticality levels of information processed by these servers and certification complexity. The AISD domain communicates with the Passenger Information and Entertainment services domain (PIESD) through a firewall to prevent unauthorized access from the PIESD. The PIESD consists of an IP LAN that connects the Embedded IFE functions, Passenger Internet portal, Onboard Passenger web, and Passenger device interface. Connectivity to off-board services from AISD and PIESD are provided through the Ethernet Switch located within ACD. This permits management of shared network resources by network devices with highest criticality levels to assure security and QoS for essential functions.

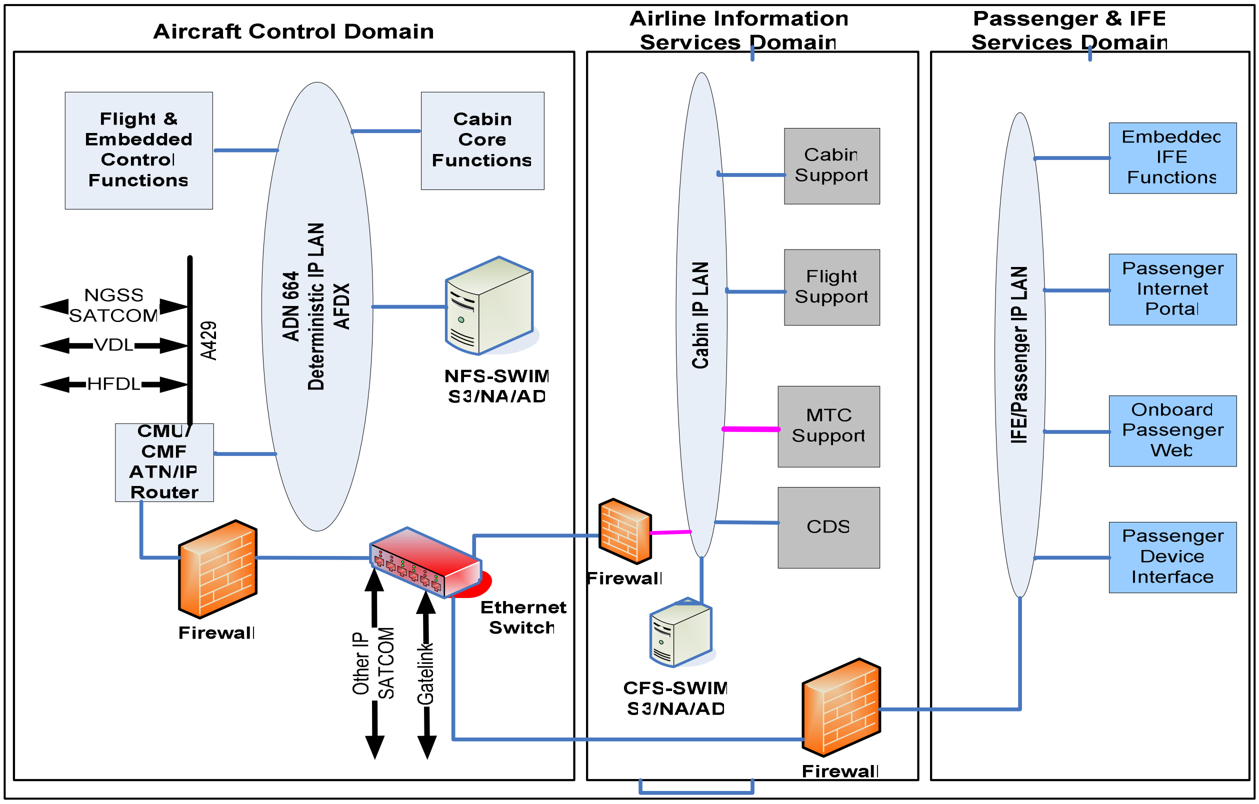

Figure 22 Vision State Avionics Architecture

Different domains in the vision state support different traffic types having different performance requirements. Each domain groups entities with similar QoS characteristics. The QoS characteristics are then applied to distinguish between different traffic types and to apply communication resources to satisfy their respective performance requirements.

The standard IP QoS has two architectural QoS models: guaranteed Internet service and differentiated Internet service. Guaranteed end-to-end Internet service is provided by the Integrated Services (IntServ) Architecture. IntServ is a connection-oriented QoS in which the QoS level is setup through a signaling protocol, called the Resource reservation Protocol (RSVP). In the vision state architecture, IntServ could be used for providing QoS only on the edge of each domain for admission control purposes because IntServ is not scalable and requires complex signaling mechanisms.

The Differentiated Services (DiffServ) Architecture allows users to choose the performance level for their needs. It is a connectionless QoS that does not guarantee end-to-end performance because intermediate devices may not support the chosen QoS. However, avionics systems within MCNA have pre-defined data flows that permit selection of intermediate devices and semi-static routes based on expected network behaviors to provide a guaranteed end-to-end QoS level. Therefore, DiffServ is recommended for all AISD domain actions other than domain admission control, and for PIESD.

The vision state architecture protects the on-board domains from unauthorized external access through a reference security model that uses firewalls and cryptographic techniques. Firewalls, as described in ARINC 664, focuses on network layer security and provide the first level of protection. Additional security mechanisms, based on the ATN security framework, are recommended by ARINC 664 to provide end-to-end data integrity, peer-entity authentication and encryption services. The ATN security framework uses Public Key Infrastructure (PKI), and industry-standard cryptographic algorithms that are implemented at the application layer. The ATN security framework is recommended for the ACD. The AISD and PIESD may employ standard IPSEC mechanisms to provide similar security services where interaction with other COTS IP networks and systems will be required. It should be noted that the standard RSA certificates used for IPSEC may consume substantial portion of the limited air/ground network bandwidth. Also, the Virtual Private Network (VPN) approach of IPSEC is inefficient for highly mobile aeronautical environment because it forces routing of data through home domain of the mobile entity. Therefore, it is recommended that the ATN security framework be adopted for all avionics domains. A single security solution will also simplify avionics implementations and key management. The NFS entity should be the central security manager for a single security solution using the ATN security framework. If interoperability requirements drive both ATN and IPSEC implementations on an aircraft, it is recommended that the NFS provide ATN-based security for the ACD while IPSEC is restricted to AISD and PIESD, which are served by the CFS.

4.3.2.1 On-board Network Protocols

The AFDX protocol, which is a special case of the profiled IP specified in Part 7 of the ARINC 664 standard, should be used for ACD. AFDX is a deterministic network that guarantees bounded delay-jitter distribution for packet delivery assuming asynchronous end systems and bounded packet arrival distribution. It replicates the performance of point-to-point wired ARINC 429 bus with unidirectional virtual links (VL). The determinism is achieved by bounding both the bandwidth and the packet delivery interval for each VL. AFDX allows network resource allocation based on the criticality of application and devices. AFDX follow a star topology of the Ethernet switches, which can be scaled by cascaded star topology. AFDX provides an ordinal integrity mechanism for frames within a VL. As AFDX has been approved to interconnect safety-critical avionics systems for the Airbus 380, it is a natural choice to provide the same functionality in future SWIM-enabled aircraft.

Tactical ATC functionality over data link requires that the aircraft be in communications with the ground systems through all phases of flight. This requirement implies that at least two disjoint paths should exist between the aircraft and the peer ATC ground system such that alternate data communication means are always available in case of one data link failure. Current air/ground protocols (ACARS and ATN) support multiple, simultaneous connections between the airborne and the ground peer entities. The CMF/routers dynamically manage these air/ground links and route data over one or more connections based on the QoS, cost, security, traffic type, and policy of the aircraft operator. Similar capabilities will be required for IP if it is to be used for ATS. A major challenge for the airborne IP router is to provide multi-homing, and local policy based routing capabilities that enable packet-by-packet control of next-hop forwarding decisions. ARINC 664 recommends Mobile IP or Host Identity Protocol (HIP) for mobility management, which decouples the mobile host computer identity and its current IP address. HIP maintains end-to-end communications between a host and its applications through use of a host's identity. Although HIP is preferred since it is adaptable and scalable, additional specification will be required for policy based routing over multiple, simultaneous data links.

4.3.2.2 Core-Net (or equivalent)

On board networks within ACD and AISD can be implemented as either one physically integrated network or two different physically-separate networks. Having physical separation simplifies security and protection rules to be applied. In addition, it may reduce cost of certification and upgrades. On the other hand, having one fully integrated network can improve the overall system maintainability and logistics as well as reduce installation cost. However, an integrated network may impose extra cost of upgraded certification of all AISD devices and applications from DO-178B level D to, potentially, DO-178B level A. The increased requirements come about because these devices may interact with flight-critical devices within the ACD. A thorough cost/benefit study is needed to address the tradeoff between these two architectural implementations. The conclusion of this study should give us a better insight of the probable implementation approach for the 2015-2020 timeframe.

The passenger network needs to be flexible and compliant to standards and state of the art consumer technologies to satisfy the needs of revenue generating passengers. Therefore, the PIESD network should be COTS, flexible, adaptive and use open IP networking standard. It is recommended that the PIESD network be physically separated from other on-board LANs with some interconnectivity to access available off-board functions.

.

4.3.2.3 Air-ground Network Interfaces

Air/ground networks can be classified into two broad categories. In the first group fall all networks that were specified or profiled by ICAO for air traffic applications. These include VDL, HFDL, Mode-S, and INMARSAT SATCOM. The ICAO-specified networks will be part of the ACD and will interface with the on-board systems through the CMF/router using ARINC 429 Williamsburg protocol. The ICAO-ATN SARPs require International Standards Organization (ISO) 8473, ISO 9542, and ISO 10747 as the air/ground network protocols. ICAO is considering IP as a subnetwork to the ATN. Even if IP is approved as an ATN subnetwork, the vision state air/ground *network layer* interface for ACD will be ATN. The second category contains the majority of air/ground networks listed in sections 2.3 and 2.4. These non-ICAO air/ground networks are intended to support non-essential services within AISD and PIESD. Some of these existing networks, such as Gatelink, IRIDIUM™, Connexion™, also use the ARINC 429 interface to communicate with the CMF/router but support IP as the air/ground protocol. They are likely to migrate to IEEE 802.3 Ethernet and IP by year 2020. Any new network is expected to adopt Ethernet/IP as the primary interface to all on-board domains.

4.3.2.4 On-board System Elements

4.3.2.4.1 Communication Management or Router Function

As discussed earlier, it is desirable that a single entity manage all air/ground network connections. This approach permits efficient, objective utilization of limited air/ground bandwidth to serve all applications having different criticality levels. Although some of the air/ground networks may not be designed to support tactical ATC messages, prioritized access to these networks from the ACD improves the overall data link availability for ATM. It is recommended that the CMF/router manage all air/ground networks in the proposed vision state architecture as shown in Figure 22.

The CMF/router should maintain priority queues for all on-board applications and grant access to the shared network resources according to applications' priority and QoS requirements. Unfortunately, this approach will only permit priority and preemption of traffic within each aircraft. It would not be possible to preempt lower priority traffic from one aircraft in favor of higher priority traffic from a different aircraft, resulting in priority inversion over the shared media. This problem can only be avoided by utilizing a network-wide, central resource manager that grants access to each aircraft based on its traffic type conveyed via the resource request. This scheme, except preemption capabilities, is implemented by VDL Mode 3, which is an ICAO-specified air/ground network specifically designed for air traffic control.

Most commercial air/ground networks have very limited priority and preemption capabilities. These networks may offer only 3 or 4 levels of priority and reserve the highest priority level for their own network management and administrative control. Therefore, aeronautical traffic types having 16 different ICAO priority levels have to be mapped to 3 levels (or less) of network priorities. Even in a centrally managed network, priority mapping will lead to priority inversion problem discussed in the previous paragraph. For example, let us assume that an air/ground network supports only 2 levels of user priorities. We can map the first 8 ICAO levels to network priority 1 and the remaining 8 ICAO levels to network priority 2. One aircraft having ICAO priority 2 traffic and another aircraft having ICAO priority 7 traffic will both map to network priority 1. However, there is a huge distinction between ICAO levels 2 and 7. If the central resource manager grants access to the second aircraft, the expected performance of the higher ICAO priority traffic from first aircraft can not be achieved. Therefore, resource allocation by a central manager will not be able to assure network access in perfect priority order unless the underlying network supports all 16 ICAO levels. This will be highly unlikely for most commercial networks.

A better strategy for shared networks will be to maintain very low aggregate utilization of the shared media and to keep the duration of each transmission short. Low utilization will minimize contention for the shared media, thus reduce retransmissions due to collisions. A fair channel access scheme coupled with short transmission time will assure that each entity will be able to access the shared media with minimal wait. By optimizing the channel utilization and transmission duration, ninety-five percentile throughput and transit delay requirements for all traffic types can be guaranteed without priority and preemption. This strategy requires an accurate model of the air/ground network to optimize the throughput-delay performance against the communications requirements. In addition, the cost penalty for underutilization of network resources should be analyzed before adaptation of this strategy. Only commercial, broadband networks appear to be suitable for this strategy at present. Additional studies should be conducted to mitigate the lack of priority support by commercial networks.

4.3.2.4.2 Network file Server

The NFS is described in ARINC Characteristic 763, Network Server System. It consists of two components: Network Service Unit (NSU) and Server Interface Unit (SIU). NSU provides common data/file storage, open system processing, application server and network communication services to devices connected through the aircraft LAN. The ARINC standard also specifies wired Ethernet and wireless connections to on-board and off-board devices. SIU provides the interfaces between NSU and other aircraft avionics equipment. The Integrated Network Server Unit (INSU) incorporates all functions of NSU and SIU packages in a single LRU device. In either configuration, the prime consideration in ARINC 763 architecture is system flexibility. Thus, it is built around industry standards and open system architectures that may be frequently and easily upgraded at a reasonable cost.

The capabilities of the network server system and the objectives of the SWIM server overlap significantly. Therefore, it is recommended that the NFS fulfill the role of airborne SWIM server.

4.3.2.4.3 SWIM Broker

The SWIM broker provides SWIM services and bridges the gap between non-SWIM enabled services and the SWIM architecture. A SWIM broker consists of application adapters (AD) to interface between Legacy Clients (LC) or Legacy Applications (LA) and SWIM Shared Services (S^3). A legacy aircraft application will exchange information with a SWIM enabled application via a SWIM-AD. The airborne SWIM server (e.g., the NFS) would cache static and less dynamic information to be provided to the aircraft without the need to consume air/ground bandwidth. It can also publish appropriate information to a terrestrial SWIM server. It is recommended that the SWIM broker function be integrated with the SWIM-enabled airborne file servers, NFS and CFS, in the vision state avionics architecture because both provide similar services.

4.3.3 System Dependencies

Aircraft and ground systems can evolve independently but they provide no user benefit without complementary enhancements to the peer system. Air traffic service providers do not realize any benefit until the number of airspace users attains a critical mass. On the other hand, aircraft operators, OEM and equipment manufacturers remain unmotivated to develop and install certification-dependent ATC functions until terrestrial supporting facilities are widely deployed and benefits are easily derived. This interdependency leads to inaction when each stakeholder waits for other entities to take the first step. Therefore, it is essential that all stakeholders commit to technology investments with a common objective that lead to defined benefits. To facilitate stakeholder commitments, a technology roadmap with incremental steps should be created to achieve the end objective. Ideally, each incremental step should provide sufficient benefits for the level of investment. Once the roadmap is defined, both aircraft operators and ATS provider should make firm commitment to perform lockstep enhancements. Cost/benefit tradeoff may not be the deciding factor for investment in NAS modernization. Aircraft equipage, on the other hand, is heavily influenced by return on investment with expected breakeven in 18 to 24 months or less, Therefore, if an incremental step does not yield sufficient benefit for the aircraft operator, the ATS provider may mandate the required capabilities or provide financial incentives to facilitate equipage. In the absence of quantifiable benefits for the aircraft operators, incentives would be the preferred option for financially strapped US air carriers.

4.3.4 Risk and Risk Mitigation Strategies

Investment interdependencies of the airborne and ground systems lead to risk-averse financial policies adopted by aircraft operators and ATS providers. The previous paragraph proposed a strategy to mitigate the financial risk. Other risks associated with the proposed vision state architecture are summarized in the following paragraphs:

- Certification Risk: All systems need to be certified for airworthiness before they can be installed on an aircraft. The level and complexity of the certification process depend on the criticality of the function performed by the airborne system. It is relatively simple to get commercial systems approved for non-essential functions. This is frequently accomplished at present. Although, a major goal of the vision state avionics architecture is to leverage commercial networks and products, it is unclear how to satisfy the certification requirements for ATM. The MCNA Certification Report [CDRL A047] provides an overview of the avionics certification process and associated issues and risks. An alternative to the current process would be to use historical performance data of the commercial network to demonstrate its reliability, integrity and robustness, thereby receive certification credit. A second alternative would be to develop an aviation-specific component of higher criticality that will envelop and isolate the commercial network elements from critical components to satisfy end-to-end safety requirements. A comprehensive study needs to be performed to recommend a strategy for certifying commercial networks for air traffic management.
- Recertification Risk: The vision state architecture relies on integrated platforms and software defined radios to improve system flexibility and adaptability. New

software may be loaded (or reconfigured by the user) to provide new communication capabilities to keep pace with evolving commercial networks. A strategy needs to be developed to permit incremental certification of systems, which is not possible under current certification process.

- Standardization Risk: The International Civil Aviation Organization (ICAO) specifies the Standards and Recommended Practices (SARPs) for air traffic communication systems to ensure global interoperability. In addition, the RTCA and/or the EUROCAE develop the Minimum Operational Performance Standards (MOPS) and the Minimum Aviation System Performance Standards (MASPs) that drive the avionics certification process[18]. Current certification practice will demand similar standards, or their equivalent, to ensure that the mobile communication networks in the vision state will meet the global interoperability and performance requirements. These aviation industry standards may become the biggest obstacle in using commercial networks because they are unlikely to meet aviation specific requirements.
- Technology Obsolescence Risk: Development of aviation industry standards is a lengthy undertaking, sometime taking up to ten years to complete. Commercial technologies evolve at a much faster pace. Therefore, it is highly likely that the aviation standards will be obsolete from commercial perspective before they can be completed. This leads to an aviation-specific implementation of mature, even aging, technology. An alternative approach to these aviation standards might be to develop a Required Communication Performance (RCP) standard and permit any commercial network for air traffic use as long as it meets the RCP. While RCP will not ensure global interoperability, compliance to ARINC 664 specification might be adequate.
- Security Risk: The Internet Protocol is the preferred mode of communication in the vision state MCNA. Connectivity to the open Internet will make the aircraft vulnerable to various network based attacks. Experiences from commercial world imply that susceptibility to these attacks can not be completely eliminated without complete, physical isolation. Therefore, it might be desirable to physically isolate the ACD network from AISD and PIESD networks. A safety/hazard analysis should be performed along with a cost/benefit analysis to justify a single network to serve all domains.
- Liability Risk: The OEM and equipment manufacturers assume some liability resulting from catastrophic failure of safety-critical avionics systems. Stringent certification and approval process may transfer some of these liabilities to the regulatory agencies. It is unclear how the liability issue will be resolved in a network centric ATM using commercial networks.

[18] The MCNA Certification Report [CDRL A047] describes how these standards are used to for avionics certification.

4.4 Avionics Transition Concepts

The MCNA Transition and Interoperability Report [CDRL A043] allocates the functional and communication services to four deployment phases. These phases are: current (year 2005), near-term (2005 to 2010), mid-term (2010 to 2020) and the vision state (2020+). As the terrestrial SWIM services evolve through these deployment phases, complementary capabilities need to be incorporated in the avionics systems to fully benefit from these advancements in the ground services. However, the avionics systems have a long life-cycle and the aircraft operators are unlikely to invest in avionics upgrades unless it can be justified by a positive ROI in less than two years. Therefore, the terrestrial systems must maintain full backward compatibility with the pre-existing avionics systems to maintain the service level required for aircraft operations.

As the majority of aircraft in service today have various levels of voice and data communication capabilities, it is essential to demonstrate that the proposed vision state architecture can be achieved through an evolutionary process. Similarly, the avionics architecture should also allow incremental addition of SWIM services and communication functionalities to provide future benefits and to profit from technological advancements.

This section examines the ability of the proposed avionics architecture to mature and adapt through various deployment phases to provide a cost-effective migration to the vision state. In addition, this section recommends a few progressive steps that might facilitate transition from the current state to the end state architecture.

4.4.1 Transition Concepts

The current state of federated avionics systems rely on aviation industry standards, and sometimes proprietary technologies, to perform the desired services as described in section 4.2.1. The domain boundaries of the vision state architecture exist and the domains are physically isolated from each other. Air/ground communication capabilities are mostly constrained within the ACD although some aircraft have introduced broadband satellite data links to the AISD. The air/ground networks supporting air traffic services are managed by the CMU/CMF.

There are three fundamental differences between the current state and the vision state avionics architecture. The following paragraphs highlight these architectural differences and discuss how various airborne capabilities can be transitioned to the vision state.

a. The first divergence is related with the introduction of SWIM capabilities in the vision state via the file server systems. The file server concept has already been conceived by AEEC in ARINC standards 763 and 628. These servers are intended to provide similar services as the SWIM server. Therefore, the ARINC 763 and 628 standards can be extended easily to incorporate SWIM capabilities proposed in sections 4.3.2.4.2 and 4.3.2.4.3. The Cabin Information Network (CIN) architecture developed by AEEC is shown in

Figure 23. This architecture is consistent with the vision state. Therefore, the proposed AISD and PIESD architectures are realizable and efforts are under way to migrate the cabin systems to the vision state architecture. The NFS and the Ethernet Switch functions are allocated to the ACD although they are included in Figure 23 to illustrate the communication connectivity.

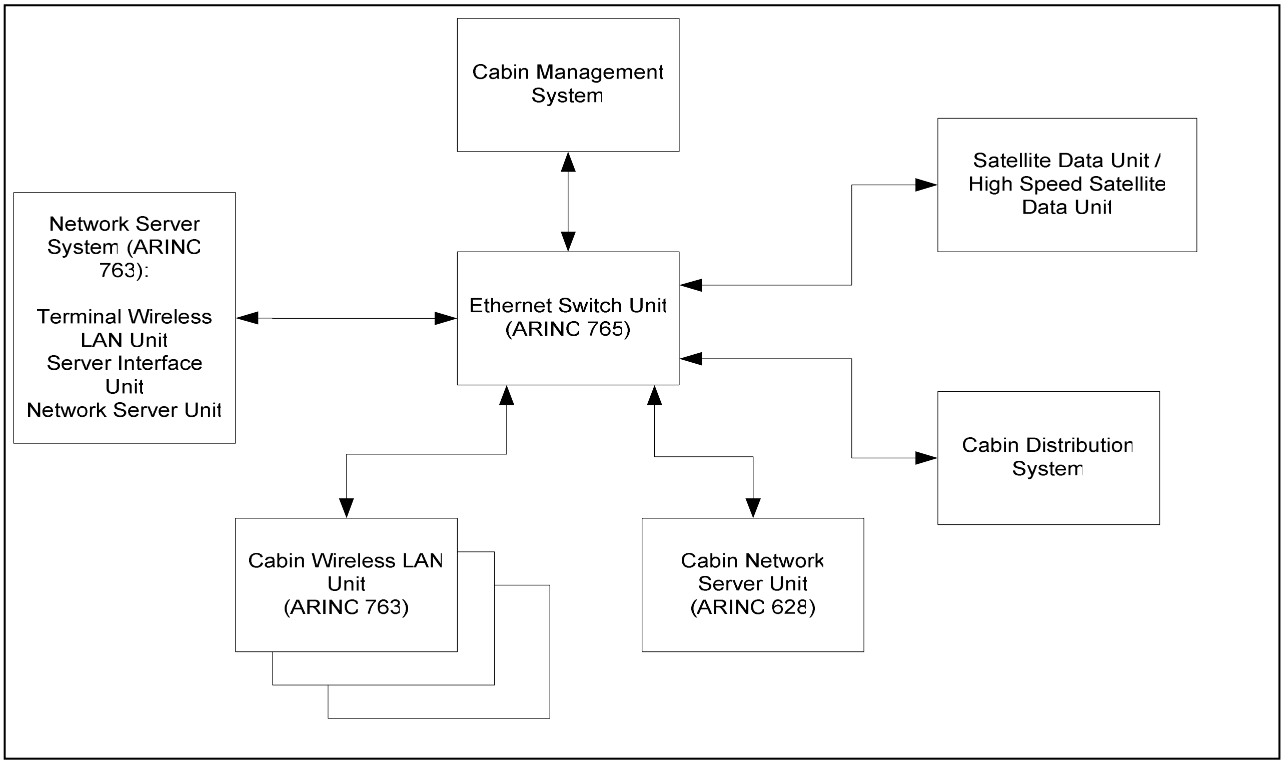

Figure 23 Cabin Information Network Architecture per AEEC

b. The second difference arises from the automation of CNS services and transition of these functionalities from voice to data link as described in the MCNA Transition and Interoperability Report [CDRL A043]. The CNS applications are specified in the ICAO ATN SARPs. Although these applications will be hosted on a small set of reconfigurable platforms in the vision state, how the datalink applications are implemented in the existing avionics configurations would impact the cost-effectiveness of the enhancements and the affordability of the aircraft operators. It should be noted that the end-to-end integrity requirement of ATN drive towards an FMS-based implementation. Unfortunately, the FMS has a higher safety and criticality level, which increases the cost of every modification of the FMS. Therefore, it would be desirable to minimize changes to the FMS through transition phases as incremental capabilities are added to the ACD. The simplest implementation option for the CNS/ATM applications is illustrated in Figure 24, where all datalink capabilities are implemented in the CMU/CMF.

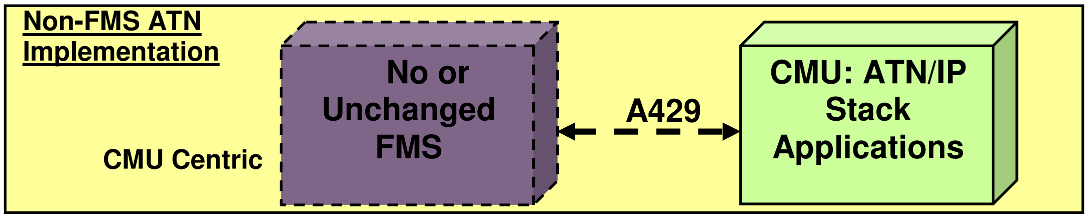

Figure 24 CMU Centric ACD Architecture for CNS/ATM Adaptation

As the MCNA CNS/ATM capabilities mature, the ATN datalink applications may be migrated to the FMS in three steps to satisfy the desired end-to-end ATN integrity requirements. These three transition steps are presented in Figure 25.

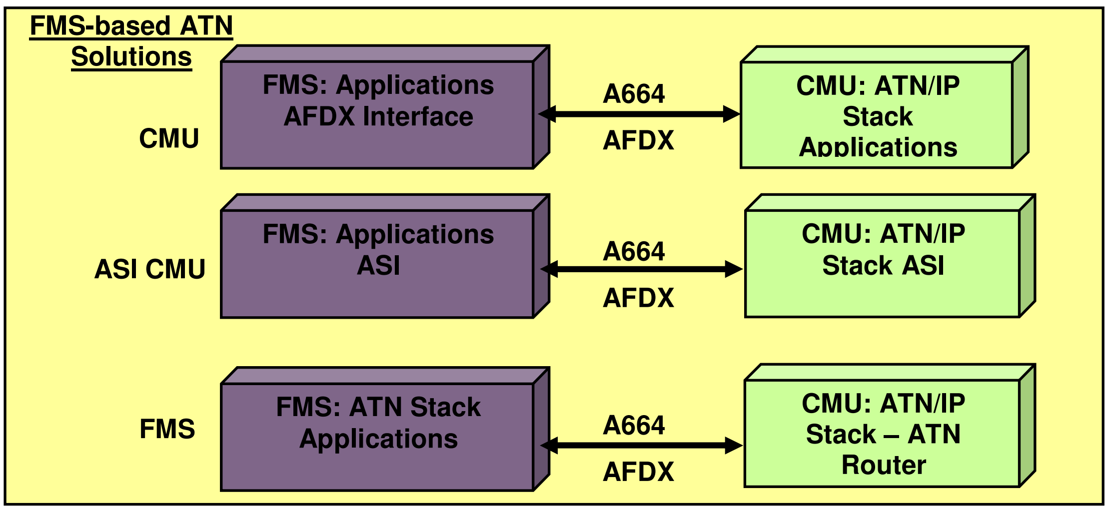

Figure 25 FMS-based ATN Implementation Alternatives

The ARINC 429 interface is replaced by the ARINC 664 AFDX /IP LAN in the first step, while maintaining the ATN applications on the CMU/CMF. The ATN Application Services Interface (ASI) is migrated to the FMS in the second step. This step might be adequate for ATN integrity because the application data will be formatted and structured by the ASI while the CMU provides the 7-layer ATN communication functions. The CMU/CMF only performs the network layer functions in the third step when the upper layer protocol functions are also migrated to the FMS. The AFDX LAN acts a subnetwork under the ATN network layer in this configuration to interconnect the ATN end-system (FMS) and the ATN router (CMU/CMF). It is recommended that the incorporation of ATN migration be restricted to the second transition step to reduce the cost and complexity of the FMS unless ICAO integrity requirements necessitate the third step.

c. The third difference between the current and the vision state architecture is the use of Internet protocol standards for on-board and off-board communications.

The proposed vision state architecture allocates management of all off-board communication functions and the air/ground network interfaces to the CMU/CMF. The isolation of these capabilities to the CMU/CMF leverages existing datalink functions of the ACD and minimizes changes to avionics systems as additional datalink technologies are introduced. As avionics and ground systems evolve from the current ACARS datalink to the ATN and the Internet, the airborne communication systems would require all three communication capabilities to maintain interoperability with terrestrial systems through the transition period. Figure 26 illustrates how various airborne applications residing in the ACD, AISD, and PIESD will access the air/ground networks through the CMU/CMF using ACARS, ATN, and IP protocols.

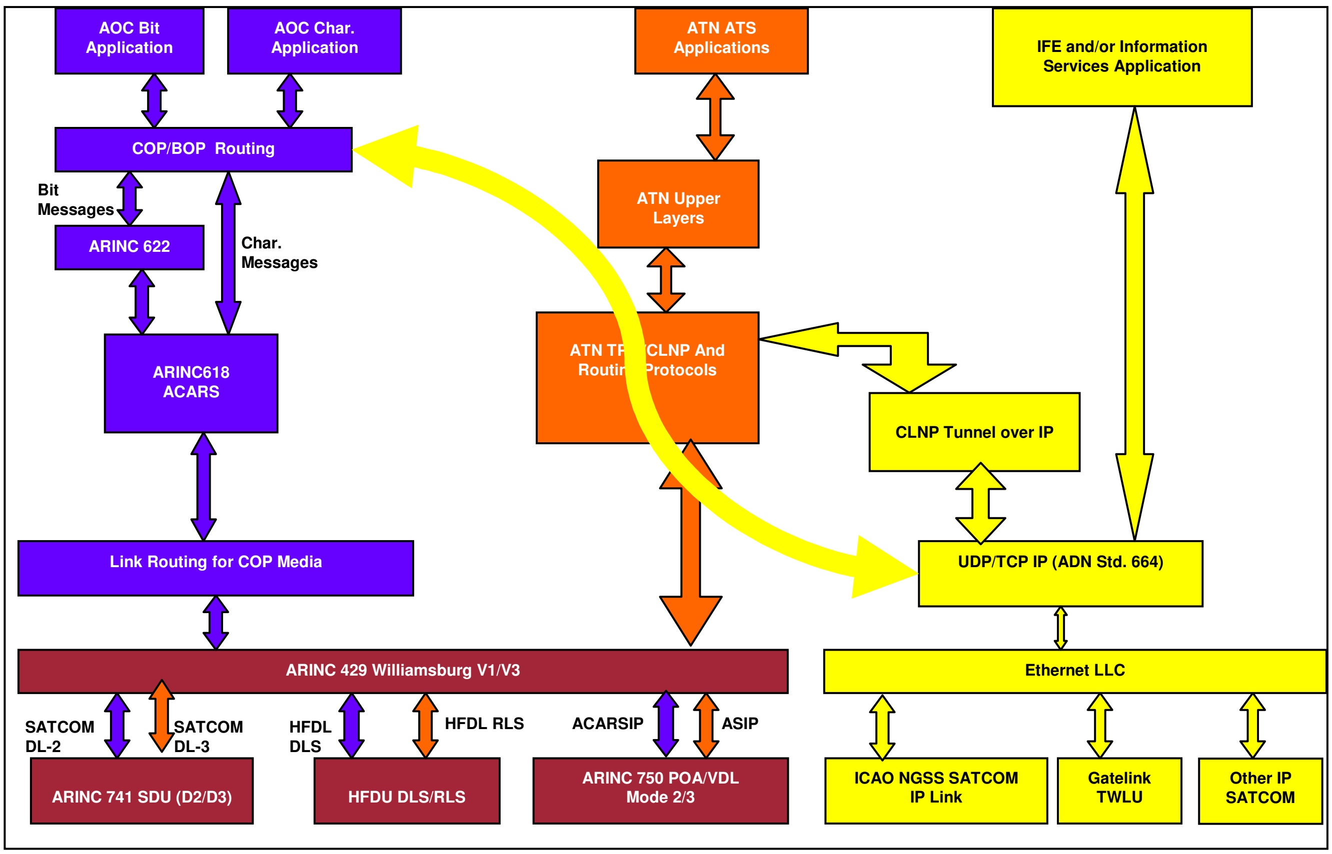

Figure 26 Data Link Protocol Transition Architecture

4.4.2 Transition Steps for SWIM Services

For cost effective transition of the avionics systems from the current state to the vision state, each transition step must provide incremental benefits to all stakeholders. It should be noted that aircraft operators are unlikely to invest without a positive ROI and breakeven within 24 months. The previous section presented a set of recommendations to transition the communication capabilities from the current state to the MCNA vision state. However, SWIM-enabled aircraft must also implement additional SWIM services on-board. Figure 27 presents an avionics transition strategy for SWIM.

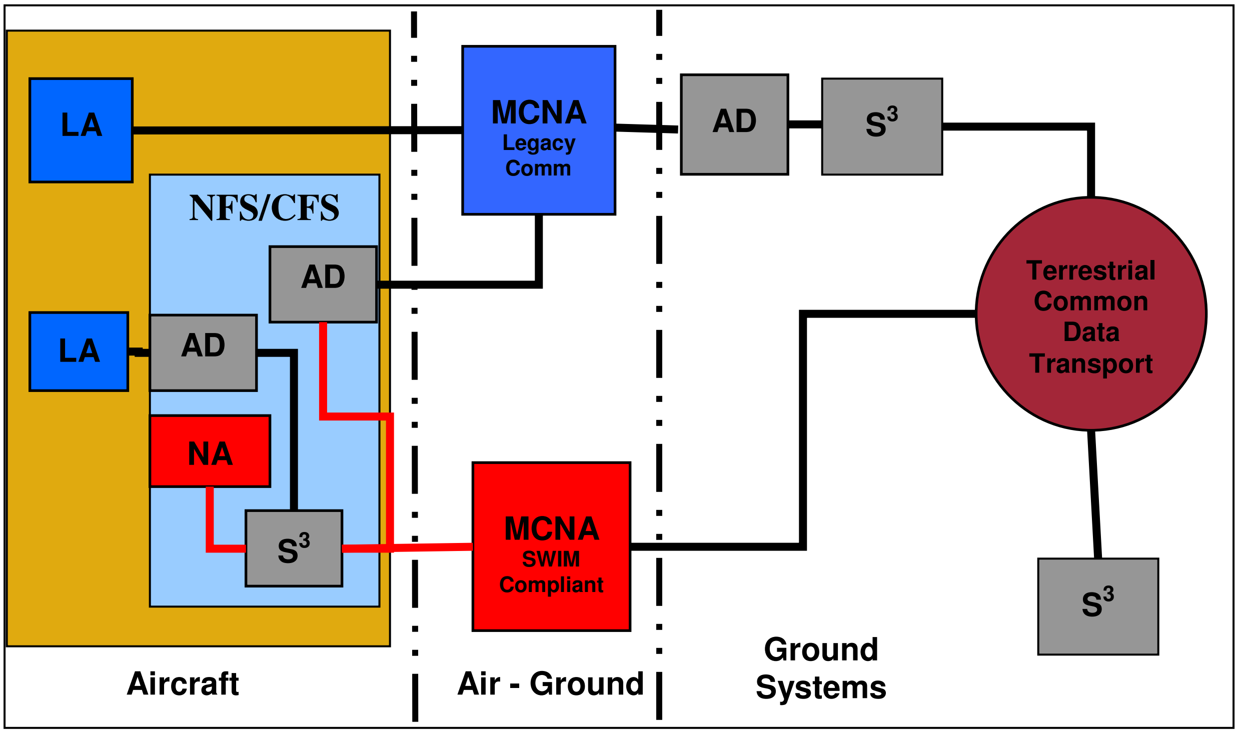

Figure 27 Avionics Transition to SWIM Services

Several variations of applications might be co-resident on an aircraft. In the current state, the Legacy, pre-SWIM Applications (LA) exchange information over legacy MCNA air/ground networks. This configuration might exist in the vision state, specifically for ACD applications. Information from/to these pre-SWIM applications will be processed by terrestrial SWIM Adapters. The first step towards SWIM equipage will depend on aircraft's need to implement Native SWIM Applications (NA). It is recommended that any new airborne application be developed as either a Native SWIM application or be adapted for SWIM. The SWIM Server (S^3) and the Adapter (AD) capabilities should be implemented on the NFS and/or the CFS at the same time when native SWIM applications are first introduced to the ACD or AISD respectively. In addition, it would be desirable to design a generic adapter function that can support most of the pre-SWIM applications. This will minimize changes to the airborne system components; thereby reducing implementation and certification costs. Once the SWIM server and the adapter capabilities are available on the aircraft, the pre-SWIM applications should access SWIM-compliant MCNA through the adapter and the SWIM server. If necessary, information from/to the native applications should be routed over legacy MCNA air/ground data links by the SWIM server as shown in Figure 27.

4.4.3 Transition Criteria

Transition of next generation aircraft, such as the AIRBUS 380 or the Boeing 787, is expected to be relatively simple because the avionics architecture for these aircraft are consistent with the ARINC 664 framework. For the retrofit aircraft, two factors dictate the introduction or modification of avionics. These are the cost of certification and implementation of a capability versus the benefits derived from it. For a successful transition, a roadmap should be created to transform the avionics architecture from the current state to the vision state in incremental steps that optimizes the cost/benefit tradeoffs. The transition should leverage any planned upgrades to minimize the implementation and certification costs. Once a transition step is completed, sufficient statistics should be collected to validate the expected cost/benefit against actual data. Future transitions steps on the roadmap should be readjusted based on the outcome of the preceding step and account for any interim technological advances. It should be noted that the transition might differ for different classes of aircraft and for different aircraft operators due to equipage variations. These variations should be factored in the cost/benefit analysis to improve the fidelity of the estimates.

4.4.4 Operation in Mixed Environment

The life cycle of avionics systems span beyond twenty years and the aircraft operators usually schedule any significant upgrades to coincide with major overhauls to reduce aircraft downtime. Therefore, some legacy aircraft would be operational in the vision state and it is likely that airborne and terrestrial systems will be in different transition stages as SWIM and MCNA capabilities evolve. This mixed operating environment can be ground into three categories:

- Aircraft with different equipage levels and at different transition steps operating within one ground system domain.
- Aircraft transitioning from one ground system to another having different SWIM capabilities.
- Aircraft communicating simultaneously with multiple ground systems having different SWIM capabilities.

Several precautions must be taken for efficient and trouble-free operation in the mixed environment. First of all, the terrestrial systems must maintain backward compatibility to ensure the quality of service to the older generation aircraft. Secondly, a signaling mechanism should be used by the airborne and ground systems to discover the capabilities of the peer entities and negotiate and/or select the greatest common SWIM service elements available. Finally, system automation should be used effectively to keep the differences transparent to the users to minimize operator workload and human errors.

4.4.5 Enabling Technologies

The avionics transition roadmap should encompass incremental technological advances as part of the overall strategy. The proposed vision state architecture accommodates all upcoming data link technologies described in section 2. Technologies that may revolutionize current aeronautical communications would be wideband radios that can simultaneously process a wide spectrum of CNS bands. This will permit further integration of RF systems beyond the SDR and integrated avionics concept presented in section 4.2.2. The current delineation of aeronautical spectrum into communication, navigation and surveillance bands needs to be studied further to determine whether a more efficient frequency allocation plan can be developed for the wideband radio concept.

4.5 Standardization

This section briefly highlights the standardization requirements for the vision state avionics architecture. This is not intended to be a comprehensive discussion of the aviation standards and certification process, which are presented in the MCNA Certification Report[19] as a standalone deliverable. The intent of this section is to identify some of the deficiencies in the existing aviation standards such that remedial actions can be undertaken.

4.5.1 Compatibility with ARINC 664

ARINC Specification 664 is primarily a guidance document that establishes the architecture framework for IP-based aircraft. It contains detailed implementation specification for AFDX, and the Ethernet physical layer. ARINC 664 also provides aeronautical profiles for IPv4 and an IP address allocation scheme using private IP address space. Except for AFDX and the Ethernet physical connectivity standards, ARINC 664 is intended to be referenced by other Airline Electronic Engineering Committee (AEEC) standards bodies as they develop ARINC implementation specifications.

The proposed vision state avionics architecture conforms to the ARINC 664 domain model. It also capitalizes on the ARINC 763 characteristics for the Network/Cabin File Server. However, none of the existing ARINC standards reflect the SWIM concept simply because these standards predate SWIM. Therefore, it would be necessary to update the relevant ARINC standards to incorporate SWIM requirements. As the NFS/CFS entities host the SWIM Server (S3), Native Application, and Adapter functions in the vision state architecture, the ARINC Characteristic 763 must be revised.

The CMU/CMF/router function within the ACD manages all air/ground network communications in the vision state architecture. The form, fit and functionality of the CMU is specified in ARINC Characteristic 758, whereas the air/ground communication protocols for ACD are defined in ARINC Specifications 637, and 618. These standards should also be amended to incorporate the required IP capabilities.

---

[19] The MCNA Certification Report [CDRL A047] describes FAA's avionics certification process and contains recommendations for amending the process for the vision state.

4.5.2 Additional Standardization effort required

The ICAO is updating the ATN SARPs to permit the use of IP as a subnetwork protocol. Once the ICAO requirements are completed, the private IPv4 addressing scheme specified in ARINC 664 may be used to provide point-to-point subnetwork connections for ATM provided Network Address Translation (NAT) function is approved by ICAO. The IPv6 addressing scheme accommodates ATN Network Service Access Point (NSAP) addresses through appropriate selection of the defined Format Prefixes. Therefore, IPv6 will permit transparent tunneling of ATN network layer protocols for mobility management and is desirable for MCNA. ARINC 664 has limited coverage of the IPv6 addressing mechanisms. This standard should be expanded to describe how IPv6 addresses will be used to support both ATN and non-ATN MCNA communications. Additional standards may also be required to deal with co-existence of IPv4 and IPv6 during the transition period.

Edition 3 of the ICAO ATN SARPs specifies cryptographic mechanisms to ensure information security. In addition to general firewall provisions, the ICAO security algorithms have been included in ARINC 664 for guidance. The AEEC Security (SEC) Working Group is currently undertaking the task of developing a Concept of Operations (ConOps) for secure aeronautical communications. The ConOps will provide the overall security framework for AOC communications. Subsequently, the AEEC sub-committees have to update their respective ARINC standards to incorporate security implementation specifications. It is anticipated that several ARINC standards, such as 618, 637, 702A, 763, 746, etc. will require modifications.

Although avionics implementations are driven by the ARINC standards, airworthiness certification of avionics is governed by the RTCA documents. As the current RTCA documents do not cover the Internet protocols, a complete suite of RTCA standards (MASPs and MOPS) may have to be developed. Alternatively, the RCP specifications may be adequate if it is used as the only criteria for approving communication systems and networks. It will not be possible to clearly identify all standardization requirements for MCNA and the vision state avionics architecture without an established certification guideline from the FAA.

5 Mapping to Requirements

This section discusses how the architecture defined in the previous sections addresses the requirements defined in the MCNA Requirements Report [26].

5.1 Functional Requirements

5.1.1 Relationship between Functions and Communication Services

The MCNA Requirements Report [26] captured the product of functional analysis that defined the first three levels of MCNA functions as summarized in Figure 28.

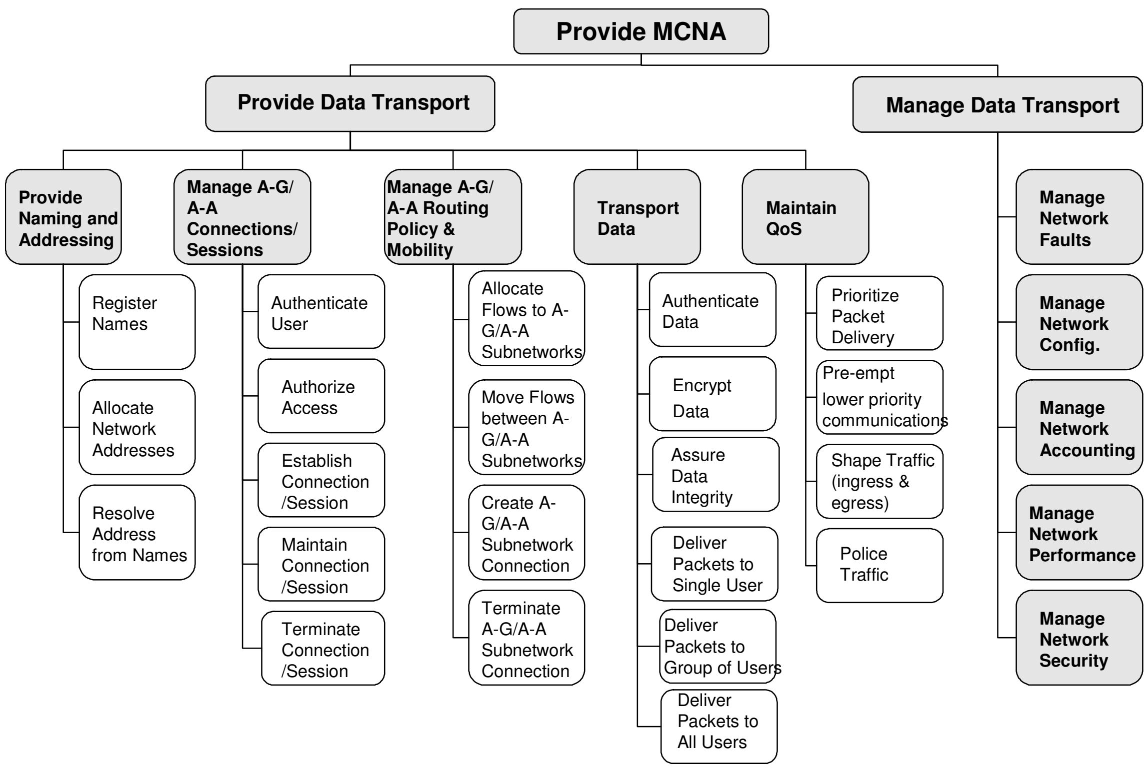

Figure 28 MCNA Functional Analysis

Also documented within this report is a set of communications services which are an extension of the RCP concept intended to comprehensively represent the aggregate of communication services required in the aviation industry. As part of the architecture analysis effort, a table was produced that maps the interaction between these MCNA functions and the MCNA communication services (Figure 29). As would typically be expected, the mapping between functions and communication services is often uneventful since most communication services require most or all of the MCNA functions.

However, a few exceptions were uncovered from this study and are listed below and highlighted in the table where possible:

- Broadcast services and Party-line voice do not need naming and addressing functions. (It should be noted that these services do not necessarily need these functions but certain implementation of these services may rely upon these functions anyway).

Function	Party-line Voice	SA Voice	Broadcast Voice	Data Messaging	Trjaecotry exchange	Broadcast to Aircraft	Broadcast From Aircraft	Ground to Air Data	Air to Ground Data	Air to Air Data	Video Exchange	Vehicle Command and Control
	Communication Services											
1.1 Provide Naming and Addressing												
1.1.1 Register mobile entities' names	N	Y	N	Y	Y	N	N	Y	Y	Y	Y	Y
1.1.2 Allocate Network Addresses	N	Y	N	Y	Y	N	N	Y	Y	Y	Y	Y
1.1.3 Resolve addresses from names	N	Y	N	Y	Y	N	N	Y	Y	Y	Y	Y
1.2 Manage A-G/A-A Links												
1.2.1 Authenticate entity (mobile user or ground station)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
1.2.2 Authorize Access	Y	Y	N	Y	Y	N	N	Y	Y	Y	Y	Y
1.2.3 Establish connection/session	Y	Y	N	Y	Y	N	N	Y	Y	Y	Y	Y
1.2.4 Maintain connection/session	Y	Y	N	Y	Y	N	N	Y	Y	Y	Y	Y
1.2.5 Handover connection/session	Y	Y	N	Y	Y	N	N	Y	Y	Y	Y	Y
1.2.6 Terminate connection/session	Y	Y	N	Y	Y	N	N	Y	Y	Y	Y	Y
1.3 Manage A-G/A-A Flows												
1.3.1 Allocate flows to A-G/A-A links	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
1.3.2 Move flows between A-G/A-A links	N	Y	N	N	N	N	N	N	N	N	Y	Y
1.4 Transport Data												
1.4.1 Authenticate data	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
1.4.2 Provide data privacy	N	Y	N	Y	Y	N	N	Y	Y	Y	Y	Y
1.4.3 Assure data integrity	N	N	N	Y	Y	P	P	Y	Y	Y	Y	Y
1.4.4 Deliver packets to a single user	N	Y	N	Y	Y	N	N	Y	Y	Y	Y	Y
1.4.5 Deliver packets to a group of users	Y	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y
1.4.6 Deliver packets to all users	N	N	Y	N	N	Y	Y	N	N	Y	N	N
1.5 Maintain QoS												
1.5.1 Prioritize packet delivery	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
1.5.2 Pre-empt lower priority communications	Y	Y	Y	N	N	N	N	N	N	N	Y	Y
1.5.3 Shape traffic (ingress and egress)	N	N	N	N	N	Y	Y	Y	Y	Y	Y	N
1.5.4 Police traffic	N	N	N	N	N	Y	Y	Y	Y	Y	Y	N

Figure 29 Mapping 1.0 Sub-Functions to the Communications Services

- Broadcast services do not require most of the session and flow management functions (which corresponds to not requiring mobility and multihoming support for these services)

- Only Selective Addressed voice, video exchange and vehicle command and control require the movement of flows between A-G and A-A links. This suggests that multihoming (if even a true requirement) is only required for these services. The limited scope of this function relates to the fact that most of these communication services are message based and do not require the long term maintenance of information flows.

- Assure data integrity is complex because the concept has different meanings for different services. Services that are voice based are far less concerned with data integrity because vocoders can handle a significant amount of loss without unacceptable performance degradation. Likewise, broadcast services will identify and drop packets with errors but the data will not be resent. This later case is an intermediate case of integrity because reliable transport is not employed but measures are taken to prevent the delivery of information that is in error. Communication services requiring this ability were marked with a "P" to reflect this function being partially required.

- Sending packets to a group of users (multicast) is a critical function to efficiently support many broadcast services.

- All services require prioritization but pre-emption does not apply to messaging services and traffic shaping and policing do not typically apply to voice services.

The network management functions apply to all services except air-air data exchange since this is really a completely unmanaged service. As such, these entries in the table were not included.

5.1.2 Relationship between Functions and Architecture Elements

Another mapping based upon MCNA functions was the allocation of functions to architecture elements. Given the representative set of architecture elements define in Section 1.2, the MCNA functions were mapped to these architecture elements as shown in Figure 30 & Figure 31. The naming and addressing functions are allocated to the hosts and routers on the aircraft and the ground, as well as the DNS. The management of A-G and A-A links is mostly allocated to ground and airborne modems. However, some of the authentication and authorization functions also extend to the routers, message routers, gateways and hosts. The management of flows is handled mostly by the routers, message routers and gateways (depending upon the implementation(s) selected to handle this capability). The transport of data is handled by the routers, message routers and gateways with the modems involved in some of the security related considerations. In QoS, the modems, routers, message routers and gateways are all involved with packet/message prioritization while the routers are responsible for traffic shaping and policing (if applicable) and the modems are responsible for pre-emption.

Function	Architecture Element												
	Airborne Firewall	Airborne Host	Airborne Modem	Airborne Router	Airborne Message Router	Airborne Gateway	Ground Station	Terrestrial Router	Terrestrial Gateway	Terrestrial Message Router	NOCC	DNS	Terrestiral Host
1.1 Provide Naming and Addressing													
1.1.1 Register mobile entities' names		X										X	
1.1.2 Allocate Network Addresses				X				X					
1.1.3 Resolve addresses from names												X	
1.2 Manage A-G/A-A Links													
1.2.1 Authenticate entity (mobile user or ground station)		X	X	X	X	X	X	X	X	X			X
1.2.2 Authorize Access			X	X	X	X	X	X	X	X			
1.2.3 Establish connection/session			X				X						
1.2.4 Maintain connection/session			X				X						
1.2.5 Handover connection/session			X				X						
1.2.6 Terminate connection/session			X				X						
1.3 Manage A-G/A-A Flows													
1.3.1 Allocate flows to A-G/A-A links				X	X	X		X	X	X			
1.3.2 Move flows between A-G/A-A links				X	X	X		X	X	X			
1.4 Transport Data													
1.4.1 Authenticate data			X	X	X	X	X	X	X	X			
1.4.2 Provide data privacy			X	X	X	X	X	X	X	X			
1.4.3 Assure data integrity			X	X	X	X	X	X	X	X			
1.4.4 Deliver packets to a single user				X	X	X		X	X	X			
1.4.5 Deliver packets to a group of users				X	X	X		X	X	X			
1.4.6 Deliver packets to all users				X	X	X		X	X	X			
1.5 Maintain QoS													
1.5.1 Prioritize packet delivery		X	X	X	X	X	X	X	X	X			X
1.5.2 Pre-empt lower priority communications			X				X						
1.5.3 Shape traffic (ingress and egress)				X				X					
1.5.4 Police traffic				X				X					

Figure 30 Allocations of 1.0 Functions to Architecture Elements

The manage data transport functions are handled by the NOCC. However, the NOCC relies upon the network elements for fault detection & reporting, configuration monitoring, performance monitoring and resource utilization reporting.

Function	Airborne Firewall	Airborne Host	Airborne Modem	Airborne Router	Airborne Message Router	Airborne Gateway	Ground Station	Terrestrial Router	Terrestrial Gateway	Terrestrial Message Router	NOCC	DNS	Terrestiral Host
	Architecture Element												
2.1 Manage Network Faults													
2.1.1 Detect Faults	X		X	X	X	X	X	X	X	X	X	X	
2.1.2 Isolate Faults											X		
2.1.3 Diagnose Faults											X		
2.1.4 Recover Faults											X		
2.1.5 Log and Notify Faults											X		
2.2 Manage Network Configuration													
2.2.1 Monitor Configuration	X		X	X	X	X	X	X	X	X	X	X	
2.2.2 Configure Networks and Services											X		
2.2.3 Process Network/Control Status Meetings											X		
2.3 Manage Network Accounting													
2.3.1 Monitor Network Resourse Utilization			X	X			X	X			X		
2.3.2 Manage Billing											X		
2.3.3 Maintain Accounting Audits											X		
2.4 Manage Network Performance													
2.4.1 Monitor Performance Data			X	X			X	X			X		
2.4.2 Analyze Performance Data											X		
2.4.3 Manage Service Quality											X		
2.4.4 Adjust Resource Utilization											X		
2.5 Manage Network Security													
2.5.1 Manage Security Attributes											X		
2.5.2 Manage Authentication											X		
2.5.3 Maintain Security Functions and Data											X		
2.5.4 Maintain Security Audits											X		

Figure 31 Allocations of 2.0 Sub-functions to Architecture Elements

5.2 Performance Requirements

The performance requirements are defined in the MCNA requirements report [26] and tied specifically to the defined communication services and levels. As these quantitative performance requirements are validated, they will be used to refine the mapping between communication service needs and the capabilities of existing and proposed candidate links. However, the network architecture is responsible for defining and regulating the performance analysis to determine how individual candidate links can be combined to achieve more aggressive communication service levels.

An example of such a performance analysis would be the following: in order to provide a communication service with very high availability, two lower availability communication systems are combined. In order to combine these systems and still meet the latency requirements, the MCNA must be capable of attempting communications over the primary link and in case of service outage, attempt communication over the backup link within latency allocation for the service. The latency characteristics of the individual links coupled with the performance requirement of the desired communication service level will determine if the MCNA architecture can establish these links sequentially, must maintain both links but attempt data transport series or if the data must be sent simultaneously over multiple links.

The performance analysis of individual system and services is a significant task. The complexity of such an effort increases greatly when multiple A-G links are combined. As such, it is important to further narrow the field of likely candidates and further define the performance requirements of services and capabilities of candidate links before seriously engaging in a comprehensive performance analysis.

6 Traceability to NAS Shortcomings and Proposed Operational Enhancements from GCNSS I

The MCNA architecture was compared against the NAS shortfalls developed during GCNSS I. Not surprisingly, the MCNA architecture, as defined in this report, addresses significant aspects of each of the defined NAS shortfalls. Recalling that MCNA, like SWIM, is an enabling technology, it is not likely to completely address shortfalls without support from other technology and/or operational enhancements. The following figures describe the seven (7) NAS shortfalls defined during GCNSS I and indicate in what manner MCNA helps to address these shortfalls (Figure 32, Figure 33, Figure 34, Figure 35, Figure 36).

The first shortfall is: a lack of timely, direct contact with aircraft in oceanic/remote domains and some low altitude domestic areas. This shortfall is further decomposed in to lack of Direct Control Pilot Communications (DCPC) and surveillance within the aforementioned airspace domains. MCNA provides ubiquitous access to CPDLC and ADS services that directly address these needs in all airspace domains with the possible exception of polar.

1	**Shortfall: Lack of timely, direct contact with aircraft in oceanic/remote domains and in some low-altitude domestic areas.**		**References and related OEP Programs**	**Impacted Domains**	**Potential MCNA Enhancement/Benefits**
	Weaknesses	**Effects**			
	a. Lack of timely Direct Controller Pilot Communications (DCPC) **b. Lack of direct surveillance of aircraft position and intent**	a. Wide separation standards (lateral and longitudinal). b. Control procedures differences at the transition between domestic and oceanic airspaces hinders efficient traffic flow. c. Inability to provide timely response to aircrew requests (altitudes, weather re-route, etc.) d. Limited knowledge of aircraft intent, hinders coordination with other traffic e. Overall reduced traffic capacity. f. Severe reductions in low altitude helicopter operations in GOM during IFR g. Use of 3rd party systems for position reports (HF is slow, 80 sec transaction times, and very low data rate, 1.8 kbps)	a. Current standard oceanic operating procedures. b. MNS-309, *Enroute/Oceanic Domain Mission Needs Statement, Apr, 2001* c. *FAA Strategic Plan for Oceanic Airspace Enhancements and Separation Reductions (Sep. 1998)* d. *Gulf of Mexico Work Group Strategic Plan (Feb 2001)* e. ER-5, *Reduce Offshore Separation* f. ER-6, *Reduce Oceanic Separation* g. ER-7, *Accommodate User Preferred Routing* h. EW-1, *Respond Effectively to Hazardous Weather* i. EW-2, *Provide Better Hazardous Weather Data*	a. Oceanic and remote regions (all altitudes) b. Offshore low-altitude regions c. Some domestic low-altitude, low-density regions	a. One of the key and initial MCNA services is data messaging. A key aspect of this service is the support of CDPLC message exchange. b. MCNA supports both the delivery of ADS-X as well as providing TIS service for the distribution of this surveillance data back to the aircraft.

Figure 32 MCNA Accommodation of GCNSS I Shortfall Number 1

The second shortfall is: ATM facilities, operators and aircraft are not "informationally integrated". This shortfall is mostly addressed by SWIM. However, MCNA addresses the integration of the aircraft into the SWIM and helps with global aspects of interoperability.

2	**Shortfall: ATM facilities, operators, and aircraft are not "informationally" integrated.**		**References and related OEP Programs**	**Impacted Domains**	**Potential MCNA Enhancement/Benefits**
	Weaknesses	**Effects**			
	a. Current information sharing is primarily ad-hoc, point-to-point data exchange **b. Limited "global" situational awareness, information not readily available to all users who could benefit from having it** **c. Manual International data exchange via telephone, teletype**	a. Response to constraints tends to be reactive rather than proactive b. Reduced capability for automated systems to aid in decision making (increased manual workload to "get data", to coordinate, etc.) c. Limited arrival/departure coordination and reduced capacity (TRACON not coordinating with neighboring sectors for efficient arrivals) d. Reduced ability to respond to current NAS status change situations e. Slow coordination between adjacent (international) facilities. Cannot presently do automated handoff between US controller and Canadian or Mexican controlle.r f. Limited availability of traffic information data to others for situational awareness g. Longer, fuel wasting taxi times during poor visibility h. Runway incursion rates remain too high	a. NAS Concept of Operations, (SWIM), 11/15/02 b. Concept of Use for NAS Wide Information Services (NWIS), FAA, 7/02 c. ER-1, *Match Airspace Design to Demands* d. ER-2, *Collaborate to Manage Congestion* e. ER-3, *Reduce Voice Communication* f. ER-5, *Reduce Offshore Separation* g. ER-6, *Reduce Oceanic Separation* h. ER-7, *Accommodate User Preferred Routing* i. ER-8, *Improve Access to SUA* j. AD-3, *Terminal Airspace and Route Redesign* k. AD-4, *Fill Gaps in Arrival and Departure Streams* l. AD-5, *Expand Use of 3-Mile Separation Standard* m. AD-6, *Coordiate for Efficient Surface Movement* n. EW-1, *Provide Better Hazardous Weather Information* o. EW-2, *Respond Effectively to Hazardous Weather*	All Domains	**a. MCNA helps extend the SWIM information sharing concept to also include the aircraft as a node** **b. MCNA addresses aspects of global situational awareness from the aspect of including the aircraft from both the perspective of an information provider and an information consumer**

Figure 33 MCNA Accommodation of GCNSS I Shortfall Number 2

The third shortfall is: information system security is fragmented. More specifically, the legacy system design impedes the introduction of an overlap security architecture and these systems have either limited or no capability to deter attacks on NAS infrastructure in the form of spoofing. MCNA introduces a coherent architecture to the air-ground portion of the NAS communications that is most vulnerable to external attack. Furthermore, MCNA provides mechanisms such as authentication and confidentiality that can directly address the existing security vulnerabilities in the NAS.

The fourth shortfall is: real-time information transfer for shared situational awareness is limited during in-flight security and emergency situations. MCNA introduces both a commercial networking architecture and sufficient bandwidth to achieve download of security video or large volumes of aircraft performance data as necessary to assist distressed aircraft. Furthermore, the use of open commercial networking standards provides a more effective means to develop and deploy ground automation applications to properly employ this data.

3	Shortfall: Information systems security is fragmented.		References and related OEP Programs	Impacted Domains	Potential MCNA Enhancement/Benefits
	Weaknesses	Effects			
	a. Legacy of existing systems designs makes it difficult to retrofit information security. **b. Almost no capability to detect/counter communications spoofing**	a. Unauthorized transmission of "fake" controller messages b. Unauthorized data access, data tampering, etc. c. Risk of potential national disruption of air traffic or loss of life due to computer attacks	a. Computer Security Act of 1987, protection of integrity, availability and confidentiality of FAA systems b. FAA Order 1370.82 implementing FAA-wide Information Systems Security Program (6/9/00) c. *Aviation Security: Vulnerabilities Still Exist in the Aviation Security System*, GAO Report, April, 2000	All Domains	a. Digitized voice provide notification/denial of unauthorized users and increased privacy b. MCNA introduces authentication, privacy and integrity mechanisms to prevent most forms of attack except denial of service (which wireless systems must go to great length to be robust via anti-jam (AJ) technology)
4	Shortfall: Real-time information transfer for shared situational awareness is limited during in-flight security or emergency situations.		References and related OEP Programs	Impacted Domains	Potential MCNA Enhancement/Benefits
	Weaknesses	Effects			
	a. Limited ability to assess security situation onboard aircraft (hijacking, terrorist attack, etc.) **b. No real-time capability to downlink large amounts of aircraft performance data during critical emergency**	a. Slow response time for national security agencies. b. Limited ability for security agencies to have situational awareness of onboard events c. Aircraft equipment experts hindered to helping to solve major problems - limited to voice exchanges between specialists and pilots.	a. Events of September 11, 2001 b. Alaska 261 accident	All Domains (primarily enroute and oceanic)	a. Video/audio direct to TSA is an MCNA communication service class under consideration b. Transfer of data to aircraft and transfer of data from aircraft support such high bandwidth applications

Figure 34 MCNA Accommodation of GCNSS I Shortfalls Number 3 & 4

The fifth shortfall is: VHF channel capacity is near limit. This is an even greater shortfall for the EU and has been a key driver of the FCS activities that MCNA is closely aligned with. MCNA is looking specifically to address this shortfall not only through the efforts outlined in FCS but also with respect to the development of an open SoS architecture that enables the rapid introduction of new air-ground technologies. As such, MCNA is a technology enabler that allows the NAS to not only catch up with spectrum demands but also more readily maintained aligned with the continuing growth of bandwidth needs within a spectrum constrained environment.

The sixth shortfall is: Radar remains the primary form of surveillance. This shortcoming results in limited surveillance coverage in certain airspace domains, as well as, high (and constantly escalating) O&M costs to maintain this aging infrastructure. Since GCNSS I, many of the political barriers toward solving this shortcoming have been removed. Recently, the community has re-established their embrace of dependant surveillance techniques for the future. With this, ADS can become the dominant form of aircraft surveillance. ADS is one of the MCNA services and provides both better surveillance accuracy and results in cheaper infrastructure that is more easily maintained.

5	**Shortfall: VHF channel capacity is near limit.**		References and related OEP Programs	Impacted Domains	Potential MCNA Enhancement/Benefits
	Weaknesses	**Effects**			
	a. Limited ability to respond to non-critical pilot requests **b. VHF spectrum for both ATS and AOC uses could "run out" before 2010.**	a. Limited ability to provide traffic and flight information for aircrew situational awareness b. High voice miscommun-ication rate and increased controller workload c. Larger miles-in-trail separation limiting enroute capacity d. Ability to use VHF for data is eventually limited	a. *White Paper: Spectrum Depletion Analysis*, MITRE, April 2003 b. Multiple analyses of Controller-to-Pilot Voice Communications, Cardosi, Burki-Cohen, 1993-96 b. *Radio Spectrum Plan for 2001-2010*, FAA, 9/30/2001 c. ER-3, *Reduce Voice Communication*	All domestic domains	a. MCNA is specifically addressing aspects of the VHF congestion problem by providing means to solve A-G communications via multiple means thus allow offload of traffic to other bands such as DME, AMSRS (ATC), and MLS. b. Looking to initially move AOC out of band to reduce ATS congestion, later followed by providing ATS services out of band as well.

6	**Shortfall: Radar remains the primary source of surveillance information.**		References and related OEP Programs	Impacted Domains	Potential MCNA Enhancement/Benefits
	Weakness	**Effects**			
	a. Loss of coverage in some low-altitude areas, some surface areas, terrain blind areas, offshore, oceanic/remote. **b. Increasing radar infrastructure Operations & Maintenance costs.**	a. Wider separation due to current radar performance (update rate, imprecise position determination from overlapping radars, display of turns lag actual change in course, etc.) b. Frequent Mode A code changing and identification ambiguities. c. Traffic routes generally limited to areas with good radar coverage. d. Not supportive of long range arrival planning efficiencies.	a. *FAA Enhanced Surveillance Capability MNS #326*, April 2001 b. AD-4 *Fill Gaps in Arrival Departure Streams* c. AD-5 *Expand Use of 3-mile Separation Std* d. AD-6 *Coordinate Efficient Surface Movement* e. ER-5/6 *Reduce Offshore/Oceanic Separation* f. ER-7 *Accommodate User Preferred Routing* g. AW-1 *Maintain Runway Use in Reduced Visibility* h. AW-2 *Space Closer to Visual Standards*	All Domains	a. Direct datalink of Automated Dependant Surveillance position and intent - Enroute (inproved accuracy, potential reduction in O&M costs) - Offshore, Oceanic/Remote - MCNA provides the means to integrate services from multiple air-ground systems to enhance global coverage of dependant surveillance b. Movement towards dependant surveillance (particularly ADS-B) would eliminate the need for costly radar infrastruture and replace with much more affordable GBT's

Figure 35 MCNA Accommodation of GCNSS I Shortfalls Number 5 & 6

The seventh and final shortfall from GCNSS I is: current procedures and tools limit the flexibility of arrival management. While this shortfall is mostly addressed via SWIM and enhanced ground automation, MCNA is also an enabling technology for key operational enhancements in arrival management. Specifically, MCNA enables the automatic upload of trajectories recommended from ground automation systems rather than imposing the requirement upon both pilots and controllers to exchange the arrival clearance via voice and have the pilots enter this clearance into the FMC.

<table>
<tr><td rowspan="2">7</td><td colspan="2"><u>Shortfall</u>: Current procedures and tools limit arrival management flexibility.</td><td rowspan="2">References
and related OEP Programs</td><td rowspan="2">Impacted Domains</td><td rowspan="2">Potential MCNA Enhancement/Benefits</td></tr>
<tr><td>Weakness</td><td>Effects</td></tr>
<tr><td></td><td>a. Airspace structure and communications restrictions restrict TRACONS's ability to work arrival plans further out in neighboring sectors.

b. Fixed routes over a few metering fixes limit flexibility.</td><td>a. Limited flexibility to manage arrival flow due to real tme constraints

b. Non-optimal aircraft performance efficiency during descent</td><td>a. RCTA Concept of Operations, Section 1.3

b. <u>AD-2</u>, Use Crossing Runway Procedures

c. <u>AD-3</u>, Redesign Terminal Airspace and Routes

d. <u>AD-4</u>, Fill Gaps in Arrival & Departure Streams

e. <u>AD-5</u>, Expand Use of 3-mile Separation

b. <u>AW-1</u>, Maintain Runway Use in Reduced Visibility</td><td>Terminal</td><td>a. MCNA integrates communication capability to all airspace domains such that a facility could negotiate trajectories with an aircraft during any phase of flight

b. MCNA supports the upload of negotiated trajectories which would introduce significant additional flexbility</td></tr>
</table>

Figure 36 MCNA Accommodation of GCNSS I Shortfall Number 7

7 CONCLUSIONS & RECOMMENDATIONS

Air-Ground and Air-Air communications within the NAS is currently diverging from a single networking protocol, ACARS, to include additional protocols such as ATN (CLNP) and eventually IP. Just the divergence between ACARS and ATN has introduced a significant interoperability issue with CPDLC that has been the focus of significant industry research and interoperability activities. As the future of NAS RF communications is researched, it is imperative that A-G and A-A communications be studied from the perspective of a system of systems. In particular, careful consideration should be given to the networking protocols associated with the candidate links.

Given the interoperability issues introduced by disparate networking protocols, attention should be applied up front regarding the intended future direction. ACARS has significant limitations that resulted, many years ago, in the decision to develop new networking protocols for CNS/ATM. These protocols, ATN, have finally been developed and are in limited deployment. However, the commercial networking world has diverged significantly from the OSI protocols (from which ATN was derived) popular in the early 1990's towards IP. With the growing demand for A-G communications in support of AOC, AAC and APC communications as well, IP should become the future networking protocol for ATM. This position is consistent with the SWIM Architecture and is slowing growing in popularity and support within the aviation industry.

Given that IP is a fundamental component of the future of air-ground communications, the candidate datalinks should be investigated and developed based upon this consideration. While multiple networking protocols exist and must be accommodated during transition, the industry will benefit in the long run from migration towards a single inter-networking protocol. Accordingly, all future candidate links should be selected or modified to assure IP support. Furthermore, efforts should be conducted in the near term to introduce aeronautical communications services for AAC, AOC and eventually ATS purposes over IP links.

Currently, the IP protocol stack has certain capability limitations which prevent it from accommodating some of the ATN requirements in the areas of multihoming, mobility and policy-based routing. While mobility is an unquestionable requirement, both multihoming and policy-based routing are design solutions that must be studied further to understand the underlying communication system requirements. Furthermore, the ATN protocols were developed to support a wide array of communication services. Many of these service classes are not yet under serious investigation for operational deployment in the foreseeable future. As such, it would seem prudent to investigate the use of IP networking protocols to provide messaging services such as ADS and CPDLC that are intended for near term operational use.

IP messaging is a commercial technology that is rapidly growing in use and popularity. Furthermore, it has been selected as a key information transport service in the initial spiral SWIM design. Applying this IP messaging capability would address the short term IP mobility issues and provide a means to handle AAC, AOC and ATS message exchanges that are currently handled via ACARS. In addition IP messaging addresses many of the immediate shortcomings of ACARS such as addressing and bandwidth efficiency. In parallel, ongoing research on IPv6 protocol extensions to address network mobility, multihoming and policy based routing should render acceptable and scalable solutions in time for these capabilities to be utilized by communication service classes requiring these functions. To assure that these protocol development efforts accommodate the needs of the aeronautical community, it would be advisable for representatives from the aeronautical community to monitor and contribute to these ongoing IETF activities.

Finally, the MCNA architecture is tightly coupled with the avionics architecture and consequently requires significant changes to the on-board network to achieve the end vision. Fortunately, many of the required changes have been addressed by AEEC 664. However, specifications from ARINC 664 only provide high level guidance. Therefore, further effort will be required to actually implement and trial some of these proposed avionics architectural concepts in order to work through the real world implementation issues that have not yet been addressed. Furthermore, many of the more specific details of the SWIM concept have only been defined recently and therefore were not addressed in ARINC 664. While the 664 architecture should accommodate SWIM on the aircraft, additional specifications will be required to assure optimum interoperability between vendor implementations.

8 REFERENCES

[1] Technology Assessments for Future Aeronautical Communications Systems, NASA CR 2005-213587, ITT Industries, Reston VA, May 2005.

[2] Eurocontrol FCS Technology Pre-Screening

[3] "Communication System Architecture Development for Air Traffic Management & Aviation Weather Dissemination, Subtask 4.6 (Develop Advanced Air Transportation Technologies (AATT) 2015 Architecture)," submitted to NASA Glenn Research Center under Contract NAS2-98002, May 2000, http://www.asc.nasa.gov/aatt/rto/RTOFinal24_5.pdf.

[4] "Evaluation of Multihoming Solutions", Martin Dunmore, Project 6Net, Project Title: IST-2001-32603, Deliverable Number: 32603/ULANC/DS/4.5.3/A1, January 2005.

[5] "Air/Ground Character Oriented Protocol Specification", ARINC 618-5, August 31, 2000

[6] Pelton, Scott, Nguyen, Dung and Rob Mead, "Boeing Datalink Strategy", Presented to Link200+ Workshop, February 15-16, 2005.

[7] "System-Wide Information Management Final Concept Development Analysis", Boeing ATM, GCNSS I Contract, D794-10135-1, March 24, 2004.

[8] "Advanced Airport Data Link" -Concept and Demonstrator Implementation for a Modern Airport Data Link, Erik Haas & Michael Schnell, ICNS Conference 2003, Annapolis, MD, May 2003.

[9] "NAS Target System Description (TSD) – Briefing to NASA's NExTNAS CNS Workshop", Ann Tedford, FAA, August 20th, 2003.

[10] FAA CATS-I Database, http://www.nas-architecture.faa.gov/cats

[11] GCNSS II, SWIM Architecture Document (SWIMAD) D794-10166-1.

[12] Aeronautical Telecommunications Manual (ATN) Comprehensive ATN Manual (CAMAL), Part I, January 1999.

[13] Aeronautical Telecommunications Manual (ATN) Comprehensive ATN Manual (CAMAL), Part II, January 1999.

[14] Aeronautical Telecommunications Manual (ATN) Comprehensive ATN Manual (CAMAL), Part III, January 1999.

[15] Aeronautical Telecommunications Manual (ATN) Comprehensive ATN Manual (CAMAL), Part IV, January 1999.

[16] The ATN SARPS, Edition 3, SubVolumes 1-9, ICAO DOC9705/AN956.

[17] “ATS Data Link Applications over ACARS Air-Ground Network, ARINC Specification 622-4, Published: October 12, 2001.

[18] Draft 3 of ARINC Specification 664: “Aircraft Data Network, Part 5 – Network Domain Characteristics And Interconnection”, Circulated for Review: October 20, 2004.

[19] Draft 3 of Project Paper 664: “Aircraft Data Network, Part 8 – Interoperation with Non-IP Protocols and Services”, Circulated for Review: January 12, 2005.

[20] Draft 7 of Supplement 2 to ARINC Specification 637: “Aeronautical Telecommunication Network (ATN) Implementation, Provisions, Protocols, and Services”, Circulated for Review: August 23, 2004.

[21] Draft 2 of Supplement 3 to ARINC Characteristic 763: Network Server Systems (NSS), Circulated for Review: June 10, 2004.

[22] Aviation Satellite Communication System Part 1: Aircraft Installation Provisions”, ARINC Characteristic 741P1-10, Published: December 24, 2003.

[23] Aviation Satellite Communication System Part 2: System Design and Equipment Functional Description”, ARINC Characteristic 741P2-7, Published: December 24, 2003.

[24] “ACARS Protocols for Avionics End Systems”, ARINC 619-1, January 27, 1997.

[25] FAA Operational Evolutions Plan (OEP) v. 7 2005 - 2015, February, 2005, http://www.faa.gov/programs/oep/

[26] GCNSS II - CDRL A046, MCNA Requirements Report, D794-10169-1 Rev A, June 1, 2005

[27] Taylor, Mark S., developer of the CDPD protocol specifications and co-author of “Internetwork Mobility, the CDPD Approach”, technical discussion.

[28] Dunmore, Martin, “Evaluation of Multihoming Solution”, 6Net Project, Deliverable # 32603/ULANC/DS/4.5.3/A1, January 2005.

[29] RFC 3257 - Stream Control Transmission Protocol Applicability Statement, L. Coene, Siemens, April 2002.

[30] RFC 3286 - An Introduction to the Stream Control Transmission Protocol (SCTP), L. Ong & J. Yoakum, May 2002.

9 ACRONYMS

A-A	Aircraft
A-G	Air Ground
A-S	Air Space
AAC	Airline Administrative Communications
AATT	Advanced Air Transportation Technologies
ACARS	Aeronautical Communications Addressing and Reporting System
ACAST	Advanced CNS Architectures and System Technologies
ACD	Aircraft Control Domain
AD	Administrative Domain
ADL	Airport Data Link
ADM	Administration
ADN	Aircraft Data Network
ADS	Automatic Dependent Surveillance
ADS-B	Automatic Dependent Surveillance Broadcast
AEEC	Airline Electronic Engineering Committee
AFDX	Aeronautical Full Duplex
AFI	Authority Format Identifier
AGUA	Aggregatable Global Unicast Address
AINSC	Aeronautical Industry Service Communication
AISD	Airline Information Services Domain
AM	Amplitude Modulation
AMSS	Aeronautical Mobile Satellite Services
ANCO	Advanced Network Centric Operations
ANFS	Aircraft Network and File Server
AOA	ACARS Over AVLC
AOC	Airline Operational Communications
AOCDL	Airline Operations Control Data Link
APC	Airline Passenger Communications
APNIC	Asia Pacific Network Information Center
ARIN	American Registry of Internet Numbers
ARQ	Automatic Repeat Request
ARS	Administrative Range Selector
ARTCC	Air Route Traffic Control Center
ASI	Application Services Interface
ASIC/RF	Application Specific Integrated Circuit Radio Frequency
ATC	Air Traffic Control
ATM	Air Traffic Management
ATM/CNS	Air Traffic Management Communication Navigation Surveillance
ATN	Aeronautical Telecommunications Network
ATS	Air Traffic Service
ATSC	Air Traffic Service Communication
AUTOMET	Automatic Meteorological Reporting
AVLC	Aviation VHF Link Control

B-VHF	Broadband VHF
BCA	Boeing Commercial Airplanes
BCD	Binary Coded Decimal
BER	Bit Error Rate
BGAN	Broadband Global Access Network
BGMP	Border Gateway Multicast Protocol
BLOS	Beyond Line of Sight
CAMAL	Comprehensive ATN Manual
CATS-I	Capability Architecture Tool Suite Internet
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
CDRL	Contract Data Requirements List
CDS	Common Display System
CDT	Common Data Transport
CFS	Cabin File Server
CIM	Common Information Management
CIN	Common Information Network
CLNP	Connectionless Network Protocol
CMF	Communication Management Functions
CMU	Communication Management Unit
CMU/CMF	Communication Management Unit Communication Management Function
CNS	Communications Navigation and Surveillance
CNS/ATM	Communication Navigation and Surveillance Air Traffic Management
CoA	Care of Address
CONUS	Continental United States
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off the Shelf
CPDLC	Controller Pilot Datalink Communication
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
CTN	Common Transport Network
CWLU	Cabin Wireless LAN Unit
DAMA	Demand Assigned Multiple Access
DARS	Digital Audio Radio Service
DCL	Departure Clearance
DCPC	Direct Controller to Pilot Communications
DES	Discrete Event Simulator
DFZ	Default Free Zone
DLS	Data Link Service
DME	Distance Measuring Equipment
DNS	Domain Name Server
DoS	Denial of Service
DSP	Datalink Service Providers
DVMRP	Distance Vector Multicast Routing Protocols
EFB	Electronic Flight Bag

EIRP	Effective Isotropic Radiated Power
ES	Extended Squitter
ESA	European Space Agency
ET	Expiration Time
EU	European Union
FAA	Federal Aviation Administration
FANS	Future Air Navigation System
FCAPS	Fault Configuration Accounting Performance Security
FCC	Federal Communications Commission
FCS	Future Communications Study
FDD	Frequency Division Duplexing
FEC	Forward Error Correction
FFBD	Functional Flow Block Diagram
FIFO	First in First Out
FIS	Flight Information Services
FMC	Flight Management Computer
FMS	Flight Management System
FTI	Future Telecommunication Infrastructure
G-G	Ground-Ground
GA	General Aviation
GBR	Great Brittan
GCNSS	Global Communication Navigation and Surveillance System
GCNSS-I	Global Communication Navigation and Surveillance System - Phase 1
GPS	Global Positioning Satellite
GRC	Glenn Research Center
GSM	Global System for Mobile
HA	Home Agent
HDLC	High-Level Data Link Control
HF	High Frequency
HFDL	High Frequency Datalink
HIP	Host Identity Protocol
IA-5	International Alphabet Number 5
IATA	International Air Transportation Association
IBM	International Business Machines
ICAO	International Civil Aviation Organization
ICNS	Integrated Communication Navigation and Surveillance
ID	Identifier
IDI	Initial Domain Identifier
IDP	Initial Domain Part
IDRP	Inter Domain Routing Protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IFE	In Flight Entertainment
IFF	Identification Friend or Foe
IFR	Instrument Flight Rules
IGMP	Internet Group Multicast Protocol

INMARSAT	International Maritime Satellite
INSU	Integrated Network Server Unit
IP	Internet Protocol
IPSec	IP Security
IS	Intermediate System
ISDN	Integrated Services Digital Network
ISM	Industrial Scientific and Medical
ISO	International Standards Organization
J2EE	Java 2 Enterprise Edition
JTIDS	Joint Tactical Information Distribution System
LA	Legacy Applications
LAAS	Legacy Area Augmentation System
LAN	Local Area Network
LC	Legacy Clients
LOC	Location
LOS	Line of Sight
LRU	Line Replaceable Units
MAC	Media Access Control
MASP	Minimum Aviation System Performance
MC-CDMA	Multiple Carrier Code Division Multiple Access
MCNA	Mobile Communication Network Architecture
MD	Maryland
MDCRS	Meterological Data Collection and Reporting System
MHz	Megahertz
MIDS	Multifunction Information Distribution System
MLD	Multicast Listener Discovery
MLS	Microwave Landing System
MOPS	Minimum Operational Performance Standards
MOSPF	Multicast Open Shortest Path First
MSG	Message
MTSAT	Multifunction Transport Satellite
MU	Management Unit
MU/CMU	Management Unit Communication Management Unit
NA	Native Application
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NCC	Network Control Center
NCO	Network Centric Operations
NFS	Network File Server
NFS/CFS	Network File Server Cabin File Server
NLA	Next Level Aggregation
NMO	Network Management and Operations
NOC	Network Operations Center
NOCC	Network Operations and Control Center
NSAP	Network Service Access Point

NSS	Network Server Systems
NSU	Network Service Unit
O&M	Operation and Maintenance
OEM	Original Equipment Manufacturer
OEP	Operational Evolution Plan
OOOI	Out, Off, On, In
OSI	Open System Interconnection
OSIE	OSI Environment
OSPF	Open Shortest Path First
PBR	Policy Based Routing
PC	Personal Computer
PHB	Per Hop Basis
PHY	Physical Layer
PIESD	Passenger Information and Entertainment Services Domain
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast Sparse Mode
PKI	Public Key Infrastructure
POA	Plain Old ACARS
PODD	Passenger Owned Devices Domain
PoP	Point of Presence
POP3	Post Office Protocol - Version 3
PP	Protection Profile
PTT	Push to Talk
QoS	Quality of Service
RCP	Required Communication Performance
RD	Routing Domains
RDF	Routing Domain Format
RF	Radio Frequency
RFC	Request For Comment
RIPE	Regional Internet Registry for Europe
RIR	Regional Internet Registry
RLS	Reliable Link Service
ROI	Return on Investment
RP	Rendezvous Point
RSA	Rivest, Shamir and Adleman Public Key Cryptosystem
RSVP	Resource Reservation Protocol
RTCA	Radio Technical Commission for Aeronautics
RTO	Research Task Order
RX	Receive
SA	Selective Addressed
SAI	Systems Architecture and Interfaces
SARPS	Standards and Recommended Practices Specification
SATCOM	Satellite Communications
SBB	Swift Broadband
SCTP	Stream Control Transport Protocol
SDLS	Satellite Data Link System

SDR	Software Defined Radios
SE	Systems Engineering
SEA	SWIM Enabled Applications
SEC	Security
SEL	NSAP Selector
SELCAL	Selective Calling
SEM	Systems Engineering Manual
SITA	Societe Internationale de Telecommunications Aeronautiques
SIU	Server Interface Unit
SLA	Site Level Aggregation
SM	Sparse Mode
SMTP	Simple Mail Transport Protocol
SNDCF	Sub Network Dependent Convergence Function
SoS	System of Systems
SoSE	System of Systems Engineering
SOW	Statement of Work
SSB	Single Side Band
SWIM	System Wide Information Management
SWIMAD	SWIM Architecture Document
SYS	System Identifier
TBD	To Be Determined
TCAS	Traffic Collision Avoidance System
TCP	Transmission Control Protocol
TCP/UDP	Transmission Control Protocol User Datagram Protocol
TDD	Time Division Duplex
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TFM-M	Traffic Flow Management Modernization
TIS	Traffic Information Service
TIS-B	Traffic Information Service Broadcast
TLA	Top Level Aggregator
TNAS	Transformation of the NAS
TP4	Transmission Protocol Class 4
TRACON	Terminal Radar Control
TRL	Technology Readiness Level
TSD	Target System Description
TWLU	Terminal Area Wireless LAN Unit
TX	Transmit
UAT	Universal Access Transceiver
UK	United Kingdom
ULP	Upper Layer Protocols
UMTS	Universal Mobile Telecommunications System
URI	Universal Resource Identifiers
URL	Uniform Resource Locator
US	United States
USDOD	United States Department of Defense

VA	Virginia
VDL	VHF Data Link
VDL-B	VDL Broadcast
VDR	VHF Digital Radios
VER	Version
VFR	Visual Flight Rules
VHF	Very High Frequency
VL	Virtual Links
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WRC2007	World Radio Conference 2007
WS	Web Services
XML	Extended Markup Language